SMALL HEIGHT AND INFINITE NON-ABELIAN EXTENSIONS

P. HABEGGER

ABSTRACT. Let E be an elliptic curve defined over $\mathbf{Q}$ and let $\mathbf{Q}(E_{\mathrm{tors}})$ denote the field generated by all torsion points of E. If E does not have complex multiplication then $\mathbf{Q}(E_{\mathrm{tors}})$ is an infinite non-abelian Galois extension of the rationals. We prove that the absolute logarithmic Weil height of an element of $\mathbf{Q}(E_{\mathrm{tors}})$ is either zero or bounded from below by a positive constant depending only on E. We also show that the Néron-Tate height has a similar gap on $E(\mathbf{Q}(E_{\mathrm{tors}}))$.

1. Introduction

By Northcott's Theorem, there are only finitely many algebraic numbers of bounded degree and bounded absolute logarithmic Weil height, or short, height. Kronecker's Theorem states that an algebraic number has height zero if and only if it is zero or a root of unity. So any non-zero element that is not a root of unity inside a fixed number field has height bounded from below uniformly by a positive real number. This height and the relevant properties are covered in greater detail in Section 2.1.

A field that is algebraic (but not necessarily of finite degree) over $\mathbf{Q}$ is said to satisfy the Bogomolov property, if zero is isolated among its height values. The property's name is motivated by the eponymous conjecture on points of small Néron-Tate height on curves of genus at least 2.

The fundamental example $h(2^{1/n}) = (\log 2)/n$ shows that $\mathbf{Q}(2^{1/2}, 2^{1/3}, \ldots)$, and so in particular the field of algebraic numbers, does not satisfy the Bogomolov property. But there are many infinite extensions which do and we will mention some known examples after stating our main results.

In this paper we first exhibit a new class of infinite non-abelian Galois extensions of $\mathbf{Q}$ with the Bogomolov property. These will be related to an elliptic curve E defined over $\mathbf{Q}$. We let E_{tors} denote the group of torsion points of E defined over an algebraic closure of $\mathbf{Q}$. The field $\mathbf{Q}(E_{\mathrm{tors}})$ is generated by the set of x- and y-coordinates of the points in E_{tors} with respect to a Weierstrass model of E with rational coefficients.

Theorem 1. *Suppose E is an elliptic curve defined over $\mathbf{Q}$. Then $\mathbf{Q}(E_{\mathrm{tors}})$ satisfies the Bogomolov property.*

The Néron-Tate height is a natural height function defined on the algebraic points of the elliptic curve E itself, we will review its definition in Section 8.1. The analog of Northcott's Theorem holds, in other words E contains only finite many points of bounded degree and bounded Néron-Tate height. Kronecker's Theorem for the Néron-Tate height is also true since $\hat{h}$ vanishes precisely on the torsion points of E.

2010 *Mathematics Subject Classification.* Primary 11G50; Secondary 11G05, 14H52, 14G40.

The second result of this paper is the analog of Theorem 1 for the Néron-Tate height. It gives an affirmation answer to a question of Baker [4] for elliptic curves defined over $\mathbf{Q}$.

Theorem 2. *Suppose E is an elliptic curve defined over $\mathbf{Q}$. There exists $\epsilon > 0$ such that if $A \in E(\mathbf{Q}(E_{\mathrm{tors}}))$ is non-torsion, then $\hat{h}(A) \geq \epsilon$.*

We now discuss how our results are related to the literature. Amoroso and Dvornicich [1] proved that all abelian extensions of $\mathbf{Q}$ satisfy the Bogomolov property. This result covers the field generated by all roots of unity. Later Amoroso and Zannier proved a more precise height lower bound [2] in the spirit of Lehmer's question. A special case of their result implies that the maximal abelian extension K^{ab} of a number field K satisfies the Bogomolov property. This statement was later refined by the same authors [3] to yield a uniform lower bound that depends only on the degree $[K : \mathbf{Q}]$.

We say that an elliptic curve defined over a field of characteristic zero has complex multiplication if it has a non-trivial endomorphism defined over an algebraic closure of the base field.

On the elliptic side, Baker [4] proved that if E is defined over K and either has complex multiplication or non-integral j-invariant, then a point in $E(K^{\mathrm{ab}})$ cannot have arbitrarily small positive Néron-Tate height. Silverman [19] proved the same conclusion with no restriction on E.

If E has complex multiplication and if all endomorphisms of E are also defined over K, then $K(E_{\mathrm{tors}})$ is an infinite abelian extension of K. In other words $K(E_{\mathrm{tors}}) \subset K^{\mathrm{ab}}$. Amoroso and Zannier's result implies that $\mathbf{Q}(E_{\mathrm{tors}})$ satisfies the Bogomolov property as this property is clearly inherited by subfields.

So for $K = \mathbf{Q}$ we recover Theorem 1 if E has complex multiplication. Under the same assumption on E, Baker's result implies Theorem 2.

Our results, however, hold when E does not have complex multiplication and is defined over $\mathbf{Q}$. In this case $\mathbf{Q}(E_{\mathrm{tors}})$ is still a Galois extension of $\mathbf{Q}$. But it is never abelian as we will see in a moment. The Galois group of this extension is sufficiently anabelian to push Theorems 1 and 2 outside the immediate range of earlier results involving abelian extensions. Indeed, if we were to assume $\mathbf{Q}(E_{\mathrm{tors}}) \subset K^{\mathrm{ab}}$ for some number field K, then $\mathrm{Gal}(\mathbf{Q}(E_{\mathrm{tors}})/\mathbf{Q})$ would contain the abelian subgroup $\mathrm{Gal}(\mathbf{Q}(E_{\mathrm{tors}})/K \cap \mathbf{Q}(E_{\mathrm{tors}})) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with index bounded by $d = [K : \mathbf{Q}]$. For an integer $N \geq 1$ we let $E[N] \subset E_{\mathrm{tors}}$ denote the subgroup of points of order dividing N. It is isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$. By Serre's Theorem [16] there exists a prime $p > d$ such that the natural Galois representation $\mathrm{Gal}(\mathbf{Q}(E_{\mathrm{tors}})/\mathbf{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. We fix an isomorphism $\mathrm{Aut}\, E[p] \cong \mathrm{GL}_2(\mathbf{F}_p)$ and conclude that $\mathrm{GL}_2(\mathbf{F}_p)$ contains an abelian subgroup of index at most d. By group theory, the $d!$-th power of a matrix in $\mathrm{GL}_2(\mathbf{F}_p)$ lies in said abelian subgroup. In particular, the matrices

$$\begin{pmatrix} 1 & d! \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ d! & 1 \end{pmatrix}$$

commute in $\mathrm{GL}_2(\mathbf{F}_p)$. This is absurd because $p \nmid d!$.

Height lower bounds are not only available for normal extensions with restricted Galois group, but also when dealing with fields that can be embedding in certain local fields. The early result of Schinzel [15] implies that $\mathbf{Q}^{\mathrm{mr}}$, the maximal totally real extension of $\mathbf{Q}$, satisfies the Bogomolov property. The Weil pairing is compatible with the action of the Galois group. From this we find that $\mathbf{Q}(E[N])$ contains a primitive N-th root of unity. So $\mathbf{Q}(E[N])$ cannot be contained in a totally real number field if $N \geq 3$.

Zhang [21] proved the analog of Schinzel's result for abelian varieties. In our case it states that $E(\mathbf{Q}^{\mathrm{mr}})$ contains only finitely many torsion points and does not contain points of arbitrarily small positive Néron-Tate height. Zhang deduced the same consequences for finite extensions of $\mathbf{Q}^{\mathrm{mr}}$. Of course, $E(\mathbf{Q}(E_{\mathrm{tors}}))$ contains infinitely many torsion points. So $\mathbf{Q}(E_{\mathrm{tors}})$ is not a finite extension of a totally real extension of $\mathbf{Q}$.

Bombieri and Zannier [8] studied the p-adic analog of Schinzel's result. They discovered that any normal algebraic extension of $\mathbf{Q}$ which admits an embedding into a finite extension L of $\mathbf{Q}_p$, the field of p-adic numbers, satisfies the Bogomolov property. Our field $\mathbf{Q}(E_{\mathrm{tors}})$ cannot lie in such an L, even if E is allowed to have complex multiplication. Indeed, otherwise we would have $\mathbf{Q}(E[p^n]) \subset L$ for all positive integers n. As above we see that $\mathbf{Q}(E[p^n])$ contains a primitive p^n-th root of unity ζ. It is known that $\mathbf{Q}_p(\zeta)/\mathbf{Q}_p$ has degree $p^{n-1}(p-1)$. So $\mathbf{Q}_p(\zeta) \subset L$ is impossible for n sufficiently large.

Baker and Petsche [5] proved the analog of Bombieri and Zannier's Theorem for elliptic curves.

We now give an overview of our proof of Theorem 1. For this let us suppose that E does not have complex multiplication. Our argument uses the decomposition of the height into local terms. Say $N \geq 1$ is an integer. The basic idea is to use two metric estimates, a non-Archimedean and an Archimedean one, in the number field $\mathbf{Q}(E[N])$.

The non-Archimedean estimate is done at places above an auxiliary prime number p where E has good supersingular reduction and where some other technical conditions are met. This prime is fixed once and for all and does not depend of N. Our approach is based on studying the representations

$$\mathrm{Gal}(\mathbf{Q}_p(E[\ell^n])/\mathbf{Q}_p) \to \mathrm{Aut}\, E[\ell^n] \quad \text{for an integer} \quad n \geq 1 \tag{1.1}$$

as ℓ varies over the prime divisors of N. If necessary, this includes $\ell = p$.

No ramification occurs when $\ell \neq p$. In this case we will obtain an explicit height lower bound swiftly using the product formula, cf. Lemma 5.1. The crucial point is that supersingularity forces the square of the Frobenius to act as a scalar on the reduction of E modulo p. A lift of this square to characteristic zero is in the center of Galois group of $\mathbf{Q}(E[\ell^n])/\mathbf{Q}$. This fact makes up for the failure of commutativity.

Ramification occurs when $\ell = p$ and this is what causes the main difficulty in the proof of Theorem 1. Here we can describe representations (1.1) using Lubin-Tate modules. Again we need that E has good supersingular reduction at p. But we can no longer rely on Frobenius and instead use Lubin-Tate theory to find a suitable replacement inside a higher ramification group. In general this substitute does not lie in the center of the Galois group. But its centralizer turns out to be sufficiently large for our purposes.

A dichotomy into an unramified and a ramified case already appeared in the original work of Amoroso-Dvornicich on abelian extensions of $\mathbf{Q}$. But our non-Archimedean estimate is significantly weaker than what one would expect in the abelian case. We cannot use it together with the product formula to deduce Theorem 1 directly. The situation is described in greater detail in the beginning of Section 7. We remedy this deficiency by treating the Archimedean places more carefully. Our second estimate is

Archimedean and relies on Bilu's Equidistribution Theorem [6] for algebraic numbers of small height.

Elkies [11] proved that E has supersingular reduction at infinitely many primes. It will suffice to work with only one p. However we must arrange, among other things, that the representation $\mathrm{Gal}(\mathbf{Q}(E_{\mathrm{tors}})/\mathbf{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. By Serre's Theorem this is true for all but finitely many p. At the moment, Elkies' Theorem is not known for elliptic curves over a general number field. So we restrict ourselves to treating elliptic curves defined over $\mathbf{Q}$.

The proof of Theorem 2 follows along similar lines as the proof of Theorem 1. We rely on a decomposition of the Néron-Tate height into local height functions. And we also split the non-Archimedean local estimates up into an unramified and a ramified case. We then use the Equidistribution Theorem of Szpiro, Ullmo, and Zhang [20] as a substitute for Bilu's result. This will not be enough since the local terms in the Néron-Tate height, unlike the local terms in the Weil height, can take negative values at non-Archimedean places. By a theorem of Chambert-Loir [9], points of small Néron-Tate height are equidistributed in a non-Archimedean sense at places of bad reduction. Alternatively, Baker and Petsche's [5] simultaneous approach to Archimedean and non-Archimedean equidistribution can also be used at this stage.

Theorems 1 and its elliptic counterpart Theorem 2 have a common reformulation in terms of the split semi-abelian variety $S = \mathbf{G}_m \times E$. A natural Néron-Tate height on $S(\overline{\mathbf{Q}})$ is given by $\hat{h}(\alpha, A) = h(\alpha) + \hat{h}(A)$ for $\alpha \in \mathbf{G}_m(\overline{\mathbf{Q}})$ and $A \in E(\overline{\mathbf{Q}})$. Then $\hat{h}$ vanishes precisely on S_{tors}, the group of all torsion points of S. As we have already seen, the Weil pairing implies $\mathbf{Q}(S_{\mathrm{tors}}) = \mathbf{Q}(E_{\mathrm{tors}})$. So our two previous theorems immediately imply the following corollary.

Corollary. *Suppose E is an elliptic curve defined over $\mathbf{Q}$ and let $S = \mathbf{G}_m \times E$. There exists $\epsilon > 0$ such that if $P \in S(\mathbf{Q}(S_{\mathrm{tors}}))$ is non-torsion, then $\hat{h}(P) \geq \epsilon$.*

Let us state some open questions and problems related to our results.

By Theorem 1 there exists $\epsilon > 0$, depending on E, such that for any non-zero $\alpha \in \mathbf{Q}(E_{\mathrm{tors}})$ that is not a root of unity we have $h(\alpha) \geq \epsilon$. It is a natural problem to determine an explicit ϵ in terms of the coefficients of a minimal Weierstrass equation of E. This problem is amenable to our method given explicit versions of the theorems of Bilu, Elkies and Serre. But an effective version of Elkies' Theorem is likely to introduce quantities depending on E. On the other hand, the author was unable to find an E and α such that $h(\alpha)$ is positive but arbitrarily small. Can one choose ϵ, implicit in Theorem 1, to be independently of E? A similar question can be raised in the context of Theorem 2.

Do Theorems 1 and 2 hold with $\mathbf{Q}(E_{\mathrm{tors}})$ replaced by a finite extension? Say $\epsilon > 0$. According to a conjecture of David, formulated for abelian varieties defined over number fields, there should exist a constant $c > 0$ depending only on E and ϵ with

$$\hat{h}(A) \geq \frac{c}{[\mathbf{Q}(E_{\mathrm{tors}})(A) : \mathbf{Q}(E_{\mathrm{tors}})]^{1+\epsilon}} \tag{1.2}$$

for all algebraic points A of E that are not torsion. This is a so-called relative Dobrowolski-type inequality. It is even expected to hold for $\epsilon = 0$ yielding a relative Lehmer-type inequality. Ratazzi [14] proved the generalization of (1.2) to elliptic curves with complex multiplication defined over a number field. Proving inequality (1.2) for elliptic curves without complex multiplication is a longstanding open problem, even with $\mathbf{Q}(E_{\rm tors})$ replaced by $\mathbf{Q}$. Variants of such estimates have interesting applications to unlikely intersections on abelian varieties and algebraic tori [10].

Suppose E' is a second elliptic curve defined over $\mathbf{Q}$ and let $F = \mathbf{Q}(E_{\rm tors}, E'_{\rm tors})$. Then David's Conjecture for the abelian variety $E \times E'$ expects that $\hat{h}(A) + \hat{h}(A')$ is bounded from below by a positive constant if at least one among $A \in E(F), A' \in E'(F)$ is not torsion. In a similar vein we ask if the field F satisfy the Bogomolov property.

We briefly discuss how this paper is organized. Section 2 deals mainly with issues of notation. In Section 3 we review the implications of Lubin-Tate theory for the Galois representation (1.1) when $\ell = p$. The local non-Archimedean estimates used in the proof of Theorem 1 are derived in Section 4. In Section 5 we obtain a preliminary height lower bound in direction of Theorem 1. It is then refined in Section 6 using a Kummerian descent argument. Bilu's Equidistribution Theorem then completes the proof that $\mathbf{Q}(E_{\rm tors})$ satisfies the Bogomolov property in Section 7. In Section 8 we turn our attention to lower bounds for the Néron-Tate height. The first half of this section contains a review of the Néron-Tate height while the second half finalizes the proof of Theorem 2.

This work was initiated at the Institute for Advanced Studies in Princeton. I thank Enrico Bombieri for the invitation and the Institute for its hospitality and financial support. It is my pleasure to thank Florian Herzig, Lars Kühne, and Martin Widmer for discussions, comments, and references. I am grateful to Laurent Berger, Clemens Fuchs, Andrew Kresch, and Gisbert Wüstholz for organizing a Workshop on p-adic Periods in Alpbach, Austria in Summer 2010. Many things I learned there proved influential for the current work. This research was partially supported by SNSF project number 124737.

2. Preliminaries on Heights and Local Fields

The group of units of a ring R is denoted by $R^\times$. The natural numbers $\mathbf{N}$ are $\{1, 2, 3, \ldots\}$.

2.1. Heights.

Let K be a number field. A place v of K is an absolute value $|\cdot|_v : K \to [0,\infty)$ whose restriction w to $\mathbf{Q}$ is either the standard complex absolute value $w = \infty$ or $w = p$, the p-adic absolute value for a prime p. In the former case we write $v|\infty$ and call v infinite or Archimedean. In the latter case we write $v|p$ or $v \nmid \infty$ and call v finite or non-Archimedean. A place is finite if and only if it satisfies the ultrametric triangle inequality. The place v uniquely determines an value on the completion K_v of K with respect to v. We use the same symbol $|\cdot|_v$ for the absolute value on K_v. The set of finite places can be identified naturally with the set of non-zero prime ideals of the ring of integers of K. The infinite places are in bijection with field embeddings $K \to \mathbf{C}$ up to complex conjugation. We define the local degree of v as $d_v = [K_v : \mathbf{Q}_w]$.

The absolute logarithmic Weil height, or short height, of $\alpha \in K$ is defined to be

$$h(\alpha) = \frac{1}{[K:\mathbf{Q}]} \sum_v d_v \log\max\{1, |\alpha|_v\} \tag{2.1}$$

where v runs over all places of K.

It is well-known that the height does not change if K is replaced by another number field containing α. Hence we have a well-defined function h with domain any algebraic closure of $\mathbf{Q}$ taking non-negative real values. Kronecker's Theorem states that $h(\alpha)$ vanishes precisely when $\alpha = 0$ or α is a root of unity. For these two statements we refer to Chapter 1.5 [7].

We list some properties of our height which we will refer to as basic height properties in the following. Our definition (2.1) implies

$$h(\alpha\beta) \leq h(\alpha) + h(\beta) \quad \text{and} \quad h(\alpha^k) = kh(\alpha) \tag{2.2}$$

if $\beta \in K$ and $k \in \mathbf{N}$. If $\zeta \in K$ is a root of unity, then $|\zeta|_v = 1$ for all places v of K. Hence $h(\zeta) = 0$ and more generally

$$h(\zeta\alpha) = h(\alpha).$$

The so-called product formula

$$\sum_v d_v \log|\alpha|_v = 0$$

holds if $\alpha \neq 0$ and is proved in Chapter 1.4 [7]. One consequence is $h(\alpha) = h(\alpha^{-1})$. Combining this equality with (2.2) we deduce

$$h(\alpha^k) = |k|h(\alpha) \quad \text{if} \quad \alpha \neq 0 \quad \text{and} \quad k \in \mathbf{Z}.$$

Finally, if α' is a conjugate over $\mathbf{Q}$ of α then $h(\alpha') = h(\alpha)$.

2.2. **Local Fields.** Say K/F is a finite Galois extension of discretely valued fields and let $w : K \to \mathbf{Z} \cup \{+\infty\}$ denote the surjective valuation. If $i \geq -1$ then

$$G_i(K/F) = \{\sigma \in \mathrm{Gal}(K/F);\ w(\sigma(a) - a) \geq i + 1 \text{ for all } a \in \mathcal{O}_K\}$$

is the i-th higher ramification group of K/F. We get a filtration

$$\mathrm{Gal}(K/F) = G_{-1}(K/F) \supset G_0(K/F) \supset G_1(K/F) \supset \cdots$$

where $G_0(K/F)$ is the inertia group of K/F.

Let p be a prime and let $\mathbf{Q}_p$ be the field of p-adic numbers with absolute value $|\cdot|_p$. Throughout this paper we work with a fixed algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$ and extend $|\cdot|_p$ to $\overline{\mathbf{Q}}_p$. We also fix once and for all a lift of the Frobenius automorphism $\varphi_p \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. For $f \in \mathbf{N}$ we write $\varphi_{p^f} = \varphi_p^f$. There is precisely one unramified extension of $\mathbf{Q}_p$ inside $\overline{\mathbf{Q}}_p$ of degree f and we call it $\mathbf{Q}_{p^f}$. We will take any finite extension of $\mathbf{Q}_p$ to be a subfield of $\overline{\mathbf{Q}}_p$.

The prime p will be fixed throughout the proof of our two theorems. For definiteness we let $\overline{\mathbf{Q}}$ denote the algebraic closure of $\mathbf{Q}$ in $\overline{\mathbf{Q}}_p$. We will consider number fields to be subfields of $\overline{\mathbf{Q}}$ and hence of $\overline{\mathbf{Q}}_p$. Say K is a finite extension of $\mathbf{Q}$. Then $|\cdot|_p$ restricts to a finite place of v of K. The completion K_v can be taken to be the closure of K inside $\overline{\mathbf{Q}}_p$. So if K is a Galois extension of $\mathbf{Q}$ one can canonically identify $\mathrm{Gal}(K_v/\mathbf{Q}_p)$ with a subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ by restricting.

If $n \geq 0$ then $\mu_{p^n} \subset \overline{\mathbf{Q}}$ denotes the group of roots of unity with order dividing p^n. Let $\mu_{p^\infty} \subset \overline{\mathbf{Q}}$ denote the group of roots of unity whose orders are a power of p. Hence μ_{p^∞} is the union of all μ_{p^n}. We write μ_∞ for all roots of unity in $\overline{\mathbf{Q}}$.

If K is a valued field, then $\mathcal{O}_K$ is its ring of integers and k_K is its residue field. The integers in $\mathbf{Q}_{p^f}$ will also be denoted by $\mathbf{Z}_{p^f}$.

We collect some basic, but useful, facts on finite extensions of the p-adics.

Lemma 2.1. *Let $F \subset \overline{\mathbf{Q}}_p$ be a finite extension of $\mathbf{Q}_p$. Let $K, L \subset \overline{\mathbf{Q}}_p$ be finite Galois extensions of F with K/F totally ramified and L/F unramified.*

(i) *We have $K \cap L = F$ and*

$$\mathrm{Gal}(KL/F) \ni \sigma \mapsto (\sigma|_K, \sigma|_L) \in \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$$

is an isomorphism of groups.

(ii) *The extension KL/K is unramified of degree $[L:F]$, and the extension KL/L is totally ramified of degree $[K:F]$.*

(iii) *Say $i \geq -1$. If $\sigma \in \mathrm{Gal}(KL/L) \cap G_i(KL/F)$ then $\sigma|_K \in G_i(K/F)$. Moreover, the induced map $\mathrm{Gal}(KL/L) \cap G_i(KL/F) \to G_i(K/F)$ is an isomorphism of groups.*

Proof. The extension $(K \cap L)/F$ is totally ramified and unramified. A totally ramified and unramified extension of local fields is trivial. So $K \cap L = F$. The second claim of part (i) is now a basic result of Galois theory.

To prove part (ii) we can use part (i) to conclude that KL/L is Galois with group isomorphic to $\mathrm{Gal}(K/F)$. In particular, KL/L is an extension of degree $e = [K:F]$. By a similar argument, KL/K is of degree $f = [L:F]$. We remark that KL/L and KL/F have the same ramification index e' since L/F is unramified. In particular, $e' \geq e$. On the other hand, $e' \leq [KL:L] = e$. So $e' = e$ and thus KL/L is totally ramified. We also conclude that KL/K is unramified. So part (ii) holds.

Let $\pi \in \mathcal{O}_K$ be a uniformizer for K. Moreover, let $x_1, \ldots, x_f \in \mathcal{O}_L$ be lifts of elements of a k_F-basis of k_L. Let us abbreviate $\mathcal{O} = \mathcal{O}_{KL}$.

Before proving (iii) we first need to establish the equality

$$\mathcal{O} = \sum_{l=0}^{e-1} \sum_{m=1}^{f} \pi^l x_m \mathcal{O}_F. \tag{2.3}$$

It follows by the argument given in the proof of Proposition II.6.8 [13].

We also use w to denote the unique extension of the surjective valuation $F \to \mathbf{Z} \cup \{+\infty\}$ to a surjective valuation $KL \to e^{-1}\mathbf{Z} \cup \{+\infty\}$.

Suppose $\sigma \in \mathrm{Gal}(KL/L) \cap G_i(KL/F)$. Then $ew(\sigma(a) - a) \geq i + 1$ for all $a \in \mathcal{O}$ because KL/F has ramification index e. Because K/F has the same ramification index we get $\sigma|_K \in G_i(K/F)$. This shows the first claim in part (iii).

The homomorphism in (iii) is injective by part (i). It remains to show that any $\sigma' \in G_i(K/F)$ lies in its image. By (i) we can find a unique lift $\sigma \in \mathrm{Gal}(KL/L)$ with $\sigma|_K = \sigma'$. It now suffices to show $\sigma \in G_i(KL/F)$.

Suppose $a \in \mathcal{O}$. By (2.3) we may write $a = \sum_{l,m} \pi^l x_m a_{lm}$ for some $a_{lm} \in \mathcal{O}_F$. We have $\sigma(a_{lm}) = a_{lm}$ and $\sigma(x_m) = x_m$ because these elements lie in L. We remark $ew(\sigma(\pi^l) - \pi^l) = ew(\sigma'(\pi^l) - \pi^l) \geq i + 1$ since $\pi \in \mathcal{O}_K$. The ultrametric inequality now gives

$$ew(\sigma(a)-a) = ew\left(\sum_{l,m}\sigma(\pi^l x_m a_{lm}) - \pi^l x_m a_{lm}\right) = ew\left(\sum_{l,m}(\sigma(\pi^l)-\pi^l)x_m a_{lm}\right)$$
$$\geq \min_{l,m} ew((\sigma(\pi^l)-\pi^l)x_m a_{lm}) \geq i+1.$$

This yields $\sigma \in G_i(KL/F)$, as desired. □

3. Supersingular Reduction and Lubin-Tate Theory

Let E be any elliptic curve defined over a field K. If $N \in \mathbf{N}$ then $[N]$ stands for the multiplication-by-N endomorphism of E. If ℓ is a prime, the ℓ-adic Tate module $T_\ell(E)$ of E is the inverse limit over $E[\ell^n]$ as n runs over the positive integers. If the characteristic of the base field is different from ℓ then $T_\ell(E)$ is a torsion free $\mathbf{Z}_\ell$-module of rank 2.

Throughout this section we work with the following objects. Let p be a prime number with $p \geq 5$ and set $q = p^2$. Suppose E elliptic curve is over $\mathbf{Q}_q$ presented by a minimal short Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}_q$. We assume that E has good supersingular reduction $\widetilde{E}$. We remark that $\widetilde{E}$ is an elliptic curve defined over $\mathbf{F}_q$. For technical reasons we shall suppose that the j-invariant of $\widetilde{E}$ is not among 0 or 1728.

The absolute Galois group of $\mathbf{Q}_q$ acts on the torsion points of E. So any prime ℓ determines a group homomorphism

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_q) \to \mathrm{Aut}_{\mathbf{Z}_\ell} T_\ell(E).$$

Let us suppose for the moment that $\ell \neq p$. Reducing modulo p induces an injective $\mathbf{Z}_\ell$-module homomorphism $T_\ell(E) \to T_\ell(\widetilde{E})$, cf. Chapter VII [18]. After extending scalars this yields an isomorphism

$$T_\ell(E) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \to T_\ell(\widetilde{E}) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$$

of $\mathbf{Q}_\ell$-vector spaces.

Recall that $\varphi_q \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_q)$ is a lift of the Frobenius automorphism. We let $\widetilde{\varphi}_q$ denote the q-Frobenius endomorphism of $\widetilde{E}$. Then the characteristic polynomial of $\rho_\ell(\varphi_q)$ considered as an automorphism of $T_\ell(E)$ equals the characteristic polynomial of the action of $\widetilde{\varphi}_q$ on $T_\ell(\widetilde{E})$. So the determinant of $\rho_\ell(\varphi_q)$ is the degree of $\widetilde{\varphi}_q$ and hence equal to q. By the Weil Conjectures for elliptic curves defined over finite fields, the trace of $\rho_\ell(\varphi_q)$ is an integer a_q which does not depend on ℓ. It satisfies $|a_q| \leq 2\sqrt{q} = 2p$ by Hasse's Theorem.

In the next lemma we use the hypothesis on supersingular reduction for the first time.

Lemma 3.1. *We have $a_q = \pm 2p$. Moreover, if ℓ is a prime with $\ell \neq p$ then $\widetilde{\varphi_q} = [a_q/2]$ and $\rho_\ell(\varphi_q) = a_q/2$.*

Proof. Because $\widetilde{E}$ is assumed to be supersingular we have $p|a_q$. We give a short proof of this well-known fact. Theorem 13.6.3 [12] implies $\widetilde{\varphi}_q^m = [p^{m'}]$ on $\widetilde{E}$ for certain positive integers m and m'. The degree of $\widetilde{\varphi}_q$ is $q = p^2$ and that of $[p]$ is also p^2. Hence $m = m'$ and $\lambda_1^m = \lambda_2^m = p^m$ where $\lambda_{1,2}$ are the eigenvalues of the action of $\widetilde{\varphi}_q$ on $T_\ell(\widetilde{E})$. Therefore, $\lambda_{1,2}/p$ are algebraic integers. But $a_q/p = (\lambda_1+\lambda_2)/p$ is rational, so $p|a_q$.

We have already seen $|a_q| \leq 2p$. So we may write $a_q = \epsilon p$ with $\epsilon \in \{0, \pm 1, \pm 2\}$. To show the first claim we will need to eliminate the cases $\epsilon = 0, \pm 1$.

The Theorem of Cayley-Hamilton implies that $\widetilde{\varphi}_q^2 - [a_q] \circ \widetilde{\varphi}_q + [q]$ taken as an endomorphism of $T_\ell(\widetilde{E})$ vanishes. Hence as an endomorphism of $\widetilde{E}$ we have

$$\widetilde{\varphi}_q^2 - [a_q] \circ \widetilde{\varphi}_q + [q] = 0. \tag{3.1}$$

Suppose we have $|\epsilon| \leq 1$. Since $[p] : \widetilde{E} \to \widetilde{E}$ is purely inseparable of degree q it follows that $u \circ [p] = \widetilde{\varphi}_q$ with u an automorphism of $\widetilde{E}$, cf. Proposition 13.5.4 [12]. Now $\widetilde{\varphi}_q^2 - [a_q] \circ \widetilde{\varphi}_q + [q] = 0$ implies $u^2 - [\epsilon] \circ u + 1 = 0$. If for example $\epsilon = 0$, then u is an automorphism of order 4. This is incompatible with $\widetilde{j} \neq 1728$ by Theorem III.10.1 [18]. If $\epsilon = \pm 1$ then u has order 6 or 3 and on consulting the same reference this contradicts $\widetilde{j} \neq 0$.

Hence $a_q = \pm 2p$ and the first claim holds.

We may thus rewrite (3.1) as $(\widetilde{\varphi}_q - [a_q/2])^2 = 0$. The endomorphism ring of $\widetilde{E}$ has no zero divisors, so $\widetilde{\varphi}_q = [a_q/2]$. This implies $\rho_\ell(\varphi_q) = [a_q/2]$ since the reduction homomorphism is injective. □

We come to the Galois theoretic analysis of torsion points on E with order a power of p. Our main tool is the theory of Lubin-Tate modules and its connection to local class field theory.

Lemma 3.2. *Say $n \in \mathbf{N}$.*

(i) *The extension $\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q$ is totally ramified and abelian of degree $(q-1)q^{n-1}$. Moreover,*

$$\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q) \cong \mathbf{Z}/(q-1)\mathbf{Z} \times (\mathbf{Z}/p^{n-1}\mathbf{Z})^2 \tag{3.2}$$

and

$$\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q(E[p^{n-1}])) \cong (\mathbf{Z}/p\mathbf{Z})^2 \quad \textit{if} \quad n \geq 2. \tag{3.3}$$

(ii) *Let k and i be integers with $1 \leq k \leq n$ and $q^{k-1} \leq i \leq q^k - 1$. The higher ramification groups are given by*

$$\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q(E[p^k])) = G_i(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q).$$

(iii) *Let $M \in \mathbf{Z}$ be coprime to p. The image of the representation* $\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q) \to \mathrm{Aut}\, E[p^n]$ *contains multiplication by M and acts transitively on torsion points of order p^n.*

Proof. An initial consequence of Lemma 3.1 is $a_q = \pm 2p$.

Let us first prove the current lemma if $a_q = 2p$. In this case we have

$$\widetilde{\varphi_q} = [p] \quad \text{on} \quad \widetilde{E}. \tag{3.4}$$

Taking $-x/y$ as a local parameter at the origin of E determines the formal group law associated to E, cf. Chapter IV [18]. We let $[p](T) \in \mathbf{Z}_q[\![T]\!]$ denote the multiplication-by-p power series, then

$$[p](T) \equiv pT \mod T^2\mathbf{Z}_q[\![T]\!]. \tag{3.5}$$

The reduction of $[p](T)$ modulo p is the multiplication-by-p power series of the formal group associated to $\widetilde{E}$. Relation (3.4) implies

$$[p](T) \equiv T^q \mod p\mathbf{Z}_q[\![T]\!].$$

This congruence and (3.5) imply that $[p](T)$ is a Lubin-Tate series, cf. Chapter V §2 and §4 [13]. It follows from the theory of as laid out in *loc. cit.* that the formal group associated to E is a Lubin-Tate $\mathbf{Z}_q$-module.

Since E has supersingular reduction, its reduction has no torsion points of order divisible by p. By Proposition VII.2.2 [18] the group of p^n-division points of said Lubin-Tate module is isomorphic to $E[p^n]$. Moreover, this isomorphism is compatible with the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_q)$ and we will henceforth identify the two groups.

Theorem V.5.4 [13] implies that $\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q$ is totally ramified and of degree $(q-1)q^{n-1}$. The same result stipulates that $\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q)$ is isomorphic to $\mathbf{Z}_q^\times/\mathbf{Z}_q^{(n)}$ with $\mathbf{Z}_q^{(n)}$ the n-th higher unit group of $\mathbf{Z}_q$. Let us consider the short exact sequence

$$1 \to \mathbf{Z}_q^{(1)}/\mathbf{Z}_q^{(n)} \to \mathbf{Z}_q^\times/\mathbf{Z}_q^{(n)} \to \mathbf{Z}_q^\times/\mathbf{Z}_q^{(1)} \to 1.$$

The group $\mathbf{Z}_q^{(1)}/\mathbf{Z}_q^{(n)}$ is isomorphic to $p\mathbf{Z}_q/p^n\mathbf{Z}_q \cong (\mathbf{Z}/p^{n-1}\mathbf{Z})^2$ by Proposition II.5.5 [13]. On the other hand $\mathbf{Z}_q^\times/\mathbf{Z}_q^{(1)}$ is cyclic of order $q-1$ by Proposition II.3.10 *loc. cit.* The exact sequence above splits since the groups on the outside have coprime orders. We conclude (3.2).

The Galois group in (3.3) is the kernel of the surjective homomorphism $\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q) \to \mathrm{Gal}(\mathbf{Q}_q(E[p^{n-1}])/\mathbf{Q}_q)$. Statement (3.3) now follows from (3.2) and elementary group theory. This concludes the proof of part (i) when $a_q = 2p$.

The statement on the higher ramification groups in part (ii) is Proposition V.6.1 [13].

We now come to part (iii). Both claims follow from Theorem V.5.4 [13]. Indeed we have identified $E[p^n]$ with the p^n-torsion points of the Lubin-Tate module introduced above. If $M \in \mathbf{Z}$ is coprime to p then we can also explicitly describe the field automorphism inducing multiplication by M using the local norm residue symbol from local class field theory

$$(\,\cdot\,, \mathbf{Q}_q(E[p^n])/\mathbf{Q}_q) : \mathbf{Q}_q(E[p^n])^\times \to \mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q).$$

The Theorem of Lubin and Tate, see V.5.5 [13], states that $(M^{-1}, \mathbf{Q}_q(E[p^n])/\mathbf{Q}_q)$ acts on $E[p^n]$ as multiplication by M.

The proof of the lemma is complete in the case $a_q = 2p$. We shall not neglect the case $a_q = -2p$ since this occurs if a and b happen to lie in $\mathbf{Z}_p$, cf. the example following this proof. We will reduce to the case already proved by considering a quadratic twist of E. This has the effect of flipping the sign of a_q. The details are as follows.

Because $p \neq 2$ there exists $t \in \mathbf{Z}_q$ which is not a square modulo p. In particular, $t \notin p\mathbf{Z}_q$ and $\mathbf{Q}_q(t^{1/2})/\mathbf{Q}_q$ is an unramified quadratic extension. In other words $\mathbf{Q}_q(t^{1/2}) = \mathbf{Q}_{q^2}$.

Let us consider the twist E_t of E given by $y^2 = x^3 + at^2x + bt^3$. It too has good reduction $\widetilde{E}_t$ which is a quadratic twist of $\widetilde{E}$. We note that $\widetilde{E}_t(\mathbf{F}_q) = q + 1 - a'_q$ with a'_q the trace of the q-Frobenius of $\widetilde{E}_t$. By Proposition 13.1.10 [12] we find $a'_q = -a_q = 2p$. So we may apply the current lemma to E_t.

The elliptic curves E and E_t are isomorphic over $\mathbf{Q}_{q^2}$. Indeed, $(x,y)\mapsto(tx,t^{3/2}y)$ determines an isomorphism $f:E\rightarrow E_t$. Hence

$$\mathbf{Q}_{q^2}(E_t[p^n])=\mathbf{Q}_{q^2}(E[p^n]). \tag{3.6}$$

We claim that $\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q$ is totally ramified. Recall that $\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q$ is totally ramified. Lemma 2.1(i) and (3.6) imply that the inertia degree of $\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_q$ is 2. In order to prove our claim it suffices to show that the unramified extension $\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_q(E[p^n])$ is non-trivial. For then it is of degree 2 and must account for the full residue field extension of $\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_q$. Restriction induces an isomorphism between the groups $\mathrm{Gal}(\mathbf{Q}_{q^2}(E_t[p^n])/\mathbf{Q}_q)$ and $\mathrm{Gal}(\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q)\times\mathrm{Gal}(\mathbf{Q}_{q^2}/\mathbf{Q}_q)$. So there is $\sigma\in\mathrm{Gal}(\mathbf{Q}_{q^2}(E_t[p^n])/\mathbf{Q}_q)$ with $\sigma(t^{1/2})=-t^{1/2}$. In view of statement (iii) of this lemma applied to the elliptic curve E_t we may arrange that σ acts on $E_t[p^n]$ as $[-1]$. Suppose $S=(x,y)\in E[p^n]$. Using $f(S)\in E_t[p^n]$ we find

$$[-1](f(S))=\sigma(f(S))=(\sigma(tx),\sigma(t^{3/2}y))=(t\sigma(x),-t^{3/2}\sigma(y))=[-1](f(\sigma(S)))$$

which implies $S=\sigma(S)$. So σ fixes the field $\mathbf{Q}_q(E[p^n])$. We conclude $\mathbf{Q}_q(E[p^n])\neq\mathbf{Q}_{q^2}(E[p^n])$ because σ is not trivial. Our claim from above follows and with it the first assertion of (i) for E.

By Lemma 2.1(i) restriction induces isomorphisms $\mathrm{Gal}(\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_{q^2}(E[p^k]))\rightarrow\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q(E[p^k]))$ and $\mathrm{Gal}(\mathbf{Q}_{q^2}(E_t[p^n])/\mathbf{Q}_{q^2}(E_t[p^k]))\rightarrow\mathrm{Gal}(\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q(E_t[p^k]))$ of groups for $0\leq k\leq n$. So

$$\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q(E[p^k]))\cong\mathrm{Gal}(\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q(E_t[p^k]))$$

implies the remaining assertions of part (i).

Let us prove (iii) before (ii). By what has already been shown, there is $\sigma\in\mathrm{Gal}(\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q)$ that acts on $E_t[p^n]$ as multiplication by M. We may lift σ uniquely to $\widetilde{\sigma}\in\mathrm{Gal}(\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_{q^2})$. If $S\in E[p^n]$, then $f(S)\in E_t[p^n]$. Because $\widetilde{\sigma}$ commutes with f we find that $\widetilde{\sigma}$ acts on S as multiplication by M. The first claim in part (iii) follows in general because S was arbitrary. The second claim is proved along similar lines.

Finally, we prove (ii) for E. Say $i\geq-1$. We now apply Lemma 2.1(iii) to the totally ramified extensions $\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q$ and $\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q$ and to the unramified extension $\mathbf{Q}_{q^2}/\mathbf{Q}_q$. We find isomorphisms of groups

$$\begin{tikzcd}
 & \mathrm{Gal}(\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_{q^2})\cap G_i(\mathbf{Q}_{q^2}(E[p^n])/\mathbf{Q}_q) \arrow[dl] \arrow[dr] & \\
G_i(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q) & & G_i(\mathbf{Q}_q(E_t[p^n])/\mathbf{Q}_q)
\end{tikzcd}$$

which are induced by restrictions. Part (ii) follows formally from this diagram and since f is defined over $\mathbf{Q}_{q^2}$. □

Twisting may indeed be necessary to obtain a Lubin-Tate series. To see this let us consider for the moment the case $p=5$ and elliptic curve defined by $y^2=x^3+5x+1$. It has good supersingular reduction with $a_{25}=-10$. The multiplication-by-5 power series of the associated formal group satisfies

$$[5](T)\equiv-T^{25}\mod 5\mathbf{Z}_{25}[\![T]\!].$$

It is no Lubin-Tate series because of the wrong sign. However, twisting by $\sqrt{2} \in \mathbf{Z}_{25}$ gives the Weierstrass equation $y^2 = x^3 + 10x + 2\sqrt{2}$ which leads to

$$[5](T) \equiv T^{25} \mod 5\mathbf{Z}_{25}[\![T]\!].$$

For the remainder of this section let $M \in \mathbf{N}$ be coprime to p and suppose n is a non-negative integer and $N = p^n M$. In the next lemma we collect some Galois theoretic statements on $\mathbf{Q}_q(E[N])$ which will used quite often in the current paper.

Lemma 3.3. *The following statements hold.*

(i) *The extension $\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q$ is totally ramified and $\mathbf{Q}_q(E[M])/\mathbf{Q}_q$ is unramified.*
(ii) *The composition $\mathbf{Q}_q(E[p^n])\mathbf{Q}_q(E[M])$ equals $\mathbf{Q}_q(E[N])$.*
(iii) *Restricting to $\mathbf{Q}_q(E[p^n])$ induces an isomorphism of groups*

$$\mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[M])) \to \mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q).$$

Proof. The first part of (i) follows from Lemma 3.2(i). The second part is a consequence of the basic theory of elliptic curves defined over local fields and $p \nmid M$, cf. Chapter VII [18].

Part (ii) follows since any element of $E[N]$ is the sum of an element in $E[p^n]$ and $E[M]$.

Part (iii) follows from the preceding parts and Lemma 2.1(ii). □

We state two auxiliary lemmas which are used in later sections. The first lemma describes the roots of unity in $\mathbf{Q}_q(E[N])$ having order a power of p.

Lemma 3.4. *We have $\mathbf{Q}_q(E[N]) \cap \mu_{p^\infty} = \mu_{p^n}$.*

Proof. For brevity we set $K = \mathbf{Q}_q(E[p^n])$ and $L = \mathbf{Q}_q(E[M])$. By Lemma 3.3 the extension $K/\mathbf{Q}_q$ is totally ramified, $L/\mathbf{Q}_q$ is unramified, and $KL = \mathbf{Q}_q(E[N])$.

Properties of the Weil pairing imply the inclusion "$\supset$".

To show the other inclusion we first verify

$$K \cap \mu_{p^\infty} \subset \mu_{p^n}. \tag{3.7}$$

So let ζ lie K and suppose it has order $p^{n'}$. We may assume $n' \geq n$.

If $n = 0$, then $\zeta \in \mathbf{Q}_q$. But $\mathbf{Q}_p(\zeta)/\mathbf{Q}_p$ is totally ramified by Proposition II.7.13 [13] and is only trivial if $n' = 0$. Moreover, this extension has degree $[\mathbf{Q}_q(\zeta) : \mathbf{Q}_q]$ by Lemma 2.1(ii). So we must have $n' = 0$. This proves (3.7) if $n = 0$.

We now suppose $n' \geq n \geq 1$. Restriction induces a surjective homomorphism $\mathrm{Gal}(K/\mathbf{Q}_q) \to \mathrm{Gal}(\mathbf{Q}_q(\zeta)/\mathbf{Q}_q)$. The structure of both Galois groups is known. Indeed, by Lemma 3.2(i) the group $\mathrm{Gal}(K/\mathbf{Q}_q)$ is isomorphic to $\mathbf{Z}/(q-1)\mathbf{Z} \times (\mathbf{Z}/p^{n-1}\mathbf{Z})^2$. On the other hand, $\mathrm{Gal}(\mathbf{Q}_q(\zeta)/\mathbf{Q}_q) \cong \mathrm{Gal}(\mathbf{Q}_p(\zeta)/\mathbf{Q}_p)$ as above by Proposition II.7.13. The same result also implies $\mathrm{Gal}(\mathbf{Q}_q(\zeta)/\mathbf{Q}_q) \cong (\mathbf{Z}/p^{n'}\mathbf{Z})^\times \cong \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}/p^{n'-1}\mathbf{Z}$, the second isomorphism holds since $p \neq 2$. A group homomorphism

$$\mathbf{Z}/(q-1)\mathbf{Z} \times (\mathbf{Z}/p^{n-1}\mathbf{Z})^2 \to \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}/p^{n'-1}\mathbf{Z}$$

cannot be surjective if $n' > n$. So $n' = n$. This shows that ζ has order p^n and claim (3.7) holds.

Now suppose $\zeta \in KL$ has order $p^{n'}$. Again, we may suppose $n' \geq n$. The extension KL/K is unramified by Lemma 2.1(ii), so $K(\zeta)/K$ is unramified. But ζ is contained in $\mathbf{Q}_q(E[p^{n'}]) \supset K$ by what has already been proved. The extension $\mathbf{Q}_q(E[p^{n'}])/K$ is totally ramified. Therefore, so is $K(\zeta)/K$ and hence $\zeta \in K$. Finally, we deduce $\zeta \in \mu_{p^n}$ from (3.7). □

The second lemma will play a role in a descent argument used in a later section.

Lemma 3.5. *Let us suppose $n \geq 1$. If $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$ and $\alpha \in \mathbf{Q}_q(E[N]) \smallsetminus \{0\}$ such that $\psi(\alpha)/\alpha \in \mu_\infty$, then*

$$\frac{\psi(\alpha)}{\alpha} \in \mu_{Q(n)} \quad \textit{where} \quad Q(n) = \begin{cases} q & : \textit{if } n \geq 2, \\ (q-1)q & : \textit{if } n = 1. \end{cases}$$

Proof. As in the proof of the previous lemma we write $K = \mathbf{Q}_q(E[p^n])$ and $L = \mathbf{Q}_q(E[M])$ and make use of the statements in Lemma 3.3.

Let N' denote the order of the root of unity $\psi(\alpha)/\alpha$. We decompose $N' = p^{n'}M'$ with $n' \geq 0$ and $p \nmid M'$. The root of unity $\xi = (\psi(\alpha)/\alpha)^{p^{n'}} \in KL$ has order M'. The extension $L(\xi)/L$ is totally ramified because KL/L is. The order of ξ is prime to p, so $\mathbf{Q}_p(\xi)/\mathbf{Q}_p$ is unramified by Proposition II.7.12 [13]. Hence $L(\xi)/L$ is unramified as well. We find $\xi \in L$. In particular, $\mu_{M'}$ lies in $(KL)^\psi$, the fixed field of ψ.

Recall $\xi = \psi(\alpha^{p^{n'}})/\alpha^{p^{n'}}$ has order M'. Using the Kummer map $\mathrm{Gal}(KL/(KL)^\psi) \ni \sigma \mapsto \sigma(\alpha^{p^{n'}})/\alpha^{p^{n'}}$ we find that the middle extension in

$$KL \supset (KL)^\psi(\alpha^{p^{n'}}) \supset (KL)^\psi \supset \mathbf{Q}_q(E[N/p]) \tag{3.8}$$

is cyclic of order M'.

We remark that $K/\mathbf{Q}_q(E[p^{n-1}])$ is totally ramified and $\mathbf{Q}_q(E[N/p])/\mathbf{Q}_q(E[p^{n-1}])$ is unramified. By Lemma 2.1(i), restricting to K induces an isomorphism $\mathrm{Gal}(KL/\mathbf{Q}_q(E[N/p])) \cong \mathrm{Gal}(K/\mathbf{Q}_q(E[p^{n-1}]))$.

If $n \geq 2$ then $\mathrm{Gal}(K/\mathbf{Q}_q(E[p^{n-1}])) \cong (\mathbf{Z}/p\mathbf{Z})^2$ by Lemma 3.2(i), so $\mathrm{Gal}(KL/\mathbf{Q}_q(E[N/p])) \cong (\mathbf{Z}/p\mathbf{Z})^2$ as well. We know from the discussion above that the middle extension in (3.8) is of degree M'. But M' is coprime to p, so $M' = 1$. To summarize,

$$\text{if} \quad n \geq 2 \quad \text{then} \quad \left(\frac{\psi(\alpha)}{\alpha}\right)^{p^{n'}} = 1.$$

Now let us suppose $n = 1$. Then $\mathrm{Gal}(KL/L)$ is of order $q-1$ by the same lemma. Using (3.8) we deduce $M'|q-1$. Here we find that

$$\text{if} \quad n = 1 \quad \text{then} \quad \left(\frac{\psi(\alpha)}{\alpha}\right)^{(q-1)p^{n'}} = 1.$$

If $n' = 0$ there is nothing more to show, so we will suppose $n' \geq 1$. Since $(\psi(\alpha)/\alpha)^{M'} \in KL$ has order $p^{n'}$ we have $n' \leq n$ in view of Lemma 3.4.

We define $\gamma = \alpha^{Q(n)/p}$. By the case study above $\psi(\gamma)/\gamma$ is a root of unity of order $p^{n'-1}$. So $\gamma^{p^{n'-1}} \in (KL)^\psi$ and no smaller positive power of γ lies in this field. We apply Lemma 3.4 again and use $(KL)^\psi \supset \mathbf{Q}_q(E[p^{n-1}])$ to show $(KL)^\psi \supset \mu_{p^{n-1}}$. In particular, $(KL)^\psi \supset \mu_{p^{n'-1}}$ because $n' \leq n$. Using again the Kummer map we see that $(KL)^\psi(\gamma)/(KL)^\psi$ is a cyclic extension of degree $p^{n'-1}$. The Galois group $\mathrm{Gal}(KL/(KL)^\psi)$ is a subgroup of

$\mathrm{Gal}(KL/\mathbf{Q}_q(E[N/p]))$. We have already seen above that the latter group is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^2$ if $n \geq 2$ and cyclic of order $q-1$ if $n = 1$. We conclude $n' \leq 2$ and so

$$1 = \left(\frac{\psi(\gamma)}{\gamma}\right)^p = \left(\frac{\psi(\alpha)}{\alpha}\right)^{Q(n)}. \qquad \square$$

4. Local Metric Estimates

In this section E and p are as in the previous one. Moreover, $q = p^2$ and N is a positive integer. We recall that $\varphi_q \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_q)$ is a lift of the Frobenius automorphism.

We come to a first metric estimate which is used in the unramified case $p \nmid N$.

Lemma 4.1. *If $p \nmid N$ and $\alpha \in \mathbf{Q}_q(E[N])$, then*

$$|\varphi_q(\alpha) - \alpha^q|_p \leq p^{-1} \max\{1, |\varphi_q(\alpha)|_p\} \max\{1, |\alpha|_p\}^q. \tag{4.1}$$

Proof. First say α is an integer in $L = \mathbf{Q}_q(E[N])$, i.e. $|\alpha|_q \leq 1$. Then $\varphi_q(\alpha) - \alpha^q$ is in the maximal ideal of $\mathcal{O}_L$. By Lemma 3.3(i) the extension $L/\mathbf{Q}_q$ is unramified. So said maximal ideal is $p\mathcal{O}_L$. Therefore, $|\varphi_q(\alpha) - \alpha^q|_p \leq |p|_p = p^{-1}$. In particular, (4.1) holds true.

If α is not an integer in L then α^{-1} is and we have $|\varphi_q(\alpha^{-1}) - \alpha^{-q}|_p \leq p^{-1}$. Using the ultrametric triangle inequality we bound

$$|\alpha^{-q}(\varphi_q(\alpha) - \alpha^q)|_p = |(\alpha^{-q} - \varphi_q(\alpha^{-1}))\varphi_q(\alpha)|_p \leq p^{-1}|\varphi_q(\alpha)|_p.$$

Our lemma now follows quickly. □

The second metric estimate finds application in the ramified case $p|N$.

Lemma 4.2. *If $p|N$ and $\alpha \in \mathbf{Q}_q(E[N])$, then*

$$|\psi(\alpha)^q - \alpha^q|_p \leq p^{-1} \max\{1, |\psi(\alpha)|_p\}^q \max\{1, |\alpha|_p\}^q \tag{4.2}$$

for all $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$.

Proof. For brevity we write $K = \mathbf{Q}_q(E[p^n])$ and $L = \mathbf{Q}_q(E[N/p^n])$ where $n \geq 1$ is the greatest integer with $p^n|N$.

As in the proof of Lemma 4.1 we first suppose that α is an integer in $\mathbf{Q}_q(E[N])$. We have $\psi|_K \in \mathrm{Gal}(K/\mathbf{Q}_q(E[p^{n-1}]))$. By Lemma 3.2(ii) this restriction is in $G_i(K/\mathbf{Q}_q)$ with $i = q^{n-1} - 1$. By definition we get $v(\psi(\gamma) - \gamma) \geq i + 1 = q^{n-1}$ for all integers γ in K, where v is the surjective valuation $K \to \mathbf{Z} \cup \{+\infty\}$. Lemma 3.3 implies that $\mathbf{Q}_q(E[N])/K$ is unramified. Now ψ is the unique lift of $\psi|_K$ to $\mathbf{Q}_q(E[N])$ that restricts to the identity on L. By Lemma 2.1(iii) ψ must lie in $G_i(\mathbf{Q}_q(E[N])/\mathbf{Q}_q)$. In other words

$$v(\psi(\alpha) - \alpha) \geq q^{n-1}.$$

If $\mathfrak{P}$ is the maximal ideal of the ring of integers of $\mathbf{Q}_q(E[N])$, then $\psi(\alpha) - \alpha \in \mathfrak{P}^{q^{n-1}}$. The ramification index of $\mathbf{Q}_q(E[N])/\mathbf{Q}_q$ is $e = (q-1)q^{n-1}$ by Lemmas 3.2(i) and 3.3. Therefore, $(\psi(\alpha) - \alpha)^q \in \mathfrak{P}^{qq^{n-1}} \subset \mathfrak{P}^e$. Since $p \in \mathfrak{P}^e$ we conclude

$$0 \equiv (\psi(\alpha) - \alpha)^q \equiv \psi(\alpha^q) - \alpha^q \mod \mathfrak{P}^e.$$

This leads to $|\psi(\alpha)^q - \alpha^q|_p \leq |p|_p = p^{-1}$. Hence (4.2) holds true if α is an integer in $\mathbf{Q}_q(E[N])$.

Now we suppose that α is not an integer. So α^{-1} is and we have $|\psi(\alpha^{-1})^q - \alpha^{-q}|_p \le p^{-1}$. The ultrametric triangle inequality implies

$$|\alpha^{-q}(\psi(\alpha)^q - \alpha^q)|_p = |(\alpha^{-q} - \psi(\alpha^{-1})^q)\psi(\alpha)^q|_p \le p^{-1}|\psi(\alpha)|_p^q.$$

We immediately obtain (4.2). □

5. Globalization and a First Lower Bound

We cease working over a local field and now suppose that E is an elliptic curve defined over $\mathbf{Q}$. Furthermore, $p \ge 5$ is a fixed prime and $q = p^2$

We introduce two properties associated to E and p.

(P1) The elliptic curve E has good supersingular reduction at p and the j-invariant of this reduction is not among $\{0, 1728\}$.

(P2) The natural Galois representation

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[p]$$

is surjective.

Only the first property will play a role in the current section. If it is satisfied, then the results stated in Sections 3 and 4 apply to E considered as an elliptic curve over the field $\mathbf{Q}_q$.

We recall that all our number fields are subfields of $\overline{\mathbf{Q}}_p$. Say K is a Galois extension of $\mathbf{Q}$ and let v be a place of K. An automorphism $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ determines an new place σv of K through

$$|\alpha|_{\sigma v} = |\sigma^{-1}(\alpha)|_v$$

for all $\alpha \in K$.

Let N be a positive integer. The number field $\mathbf{Q}(E[N])$ is a Galois extension of $\mathbf{Q}$.

In the unramified case we get a height lower bound without much effort.

Lemma 5.1. *Let E and p satisfy (P1). We assume $p \nmid N$. If $\alpha \in \mathbf{Q}(E[N]) \smallsetminus \mu_\infty$ is non-zero, then*

$$h(\alpha) \ge \frac{\log(p/2)}{p^2+1}.$$

Proof. Suppose ℓ is a prime divisor of N and $\ell^m|N$ with $m \in \mathbf{N}$ but $\ell^{m+1} \nmid N$. Then $\ell \ne p$ by hypothesis. Lemma 3.1 implies that φ_q acts on $E[\ell^m]$ as multiplication by $a_q/2 \in \mathbf{Z}$.

Taking the sum of points leads to a isomorphism of a direct sum of $E[\ell^m]$ with ℓ^m as above and $E[N]$. This isomorphism is compatible with the action of the Galois group. We deduce that φ_q acts on $E[N]$ as multiplication by $a_q/2$. So the restriction $\varphi_q|_{\mathbf{Q}(E[N])}$ lies in the center of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$.

The restriction of $|\cdot|_p$ to $\mathbf{Q}(E[N])$ is a place v.

We define $x = \varphi_q(\alpha) - \alpha^q \in \mathbf{Q}(E[N])$ and claim that $x \ne 0$. Indeed, otherwise we would have $h(\varphi_q(\alpha)) = h(\alpha^q)$. Conjugating does not effect the height, so $h(\alpha) = h(\alpha^q) = qh(\alpha)$ and hence $h(\alpha) = 0$. Therefore $\alpha = 0$ or $\alpha \in \mu_\infty$ by Kronecker's Theorem. This contradicts our assumption on α.

Since $x \ne 0$, the product formula implies

$$\sum_w d_w \log|x|_w = 0 \tag{5.1}$$

where the sum is over all places of $\mathbf{Q}(E[N])$.

Say w is a finite place of $\mathbf{Q}(E[N])$ above p. Then $w = \sigma^{-1}v$ for some $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ because the Galois group acts transitively on the places of $\mathbf{Q}(E[N])$ above p. The fact that φ_q and σ commute gives the second inequality in

$$|x|_w = |\sigma(\varphi_q(\alpha)) - \sigma(\alpha)^q|_v = |\varphi_q(\sigma(\alpha)) - \sigma(\alpha)^q|_p.$$

Now we estimate the right-hand side from above using Lemma 4.1 applied to $\sigma(\alpha)$

$$\begin{aligned} |x|_w &\le p^{-1}\max\{1, |\varphi_q(\sigma(\alpha))|_p\}\max\{1, |\sigma(\alpha)|_p\}^q \\ &= p^{-1}\max\{1, |\sigma(\varphi_q(\alpha))|_v\}\max\{1, |\sigma(\alpha)|_v\}^q \\ &= p^{-1}\max\{1, |\varphi_q(\alpha)|_w\}\max\{1, |\alpha|_w\}^q. \end{aligned} \tag{5.2}$$

If w is an arbitrary finite place of $\mathbf{Q}(E[N])$, the ultrametric triangle inequality gives

$$|x|_w \le \max\{|\varphi_q(\alpha)|_w, |\alpha^q|_w\} \le \max\{1, |\varphi_q(\alpha)|_w\}\max\{1, |\alpha|_w\}^q. \tag{5.3}$$

Finally, if w is an infinite place of $\mathbf{Q}(E[N])$, the triangle inequality implies

$$|x|_w \le 2\max\{|\varphi_q(\alpha)|_w, |\alpha^q|_w\} \le 2\max\{1, |\varphi_q(\alpha)|_w\}\max\{1, |\alpha|_w\}^q. \tag{5.4}$$

We apply the logarithm to the bounds (5.2), (5.3), and (5.4), take the sum over all places w of $\mathbf{Q}(E[N])$ with multiplicities d_w and use the product formula (5.1) to find

$$\begin{aligned} 0 &= \sum_{w|p} d_w \log|x|_w + \sum_{w\nmid\infty, w\nmid p} d_w \log|x|_w + \sum_{w|\infty} d_w \log|x|_w \\ &\le -\sum_{w|p} d_w \log p + \sum_{w|\infty} d_w \log 2 + \sum_{w} d_w \log(\max\{1, |\varphi_q(\alpha)|_w\}\max\{1, |\alpha|_w\}^q). \end{aligned}$$

We divide this expression by $[\mathbf{Q}(E[N]) : \mathbf{Q}]$ and use

$$\sum_{w|p} d_w = \sum_{w|\infty} d_w = [\mathbf{Q}(E[N]) : \mathbf{Q}] \tag{5.5}$$

together with the definition of the height given in Section 2.1 to obtain

$$0 \le -\log p + \log 2 + h(\varphi_q(\alpha)) + qh(\alpha).$$

Hence $h(\varphi_q(\alpha)) + qh(\alpha) \ge \log(p/2)$. The lemma follows from $h(\varphi_q(\alpha)) = h(\alpha)$, one of our basic height properties. □

The remainder of the proof of Theorem 1 concerns the study of the more delicate ramified case, i.e. when $p|N$. Instead of working with a lift of the Frobenius automorphism, we use an element in a higher ramification group. The next lemma deals with the issue that such elements need not lie in the center of the global Galois group.

Lemma 5.2. *Let E and p satisfy (P1). We assume $p|N$. Suppose $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$ which we identify with its restriction to $\mathbf{Q}(E[N])$. If*

$$G = \{\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q});\ \sigma\psi\sigma^{-1} = \psi\}$$

is its centralizer, then

$$\#Gv \ge \frac{1}{p^4}\frac{[\mathbf{Q}(E[N]) : \mathbf{Q}]}{d_v}$$

where v is the place of $\mathbf{Q}(E[N])$ determined by $|\cdot|_p$.

Proof. We define the normal subgroup

$$H = \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])).$$

of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$; it contains ψ.

We fix an isomorphism between $E[N] \cong (\mathbf{Z}/N\mathbf{Z})^2$ allowing us to represent an automorphism of $E[N]$ by an element of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. An automorphism of $E[N]$ acting trivially on $E[N/p]$ is represented by an element of $1 + N/p\mathrm{Mat}_2(\mathbf{Z}/N\mathbf{Z})$. Since the representation $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is injective, we have

$$\#H \le p^4. \tag{5.6}$$

The orbit of ψ under the action of conjugation by $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ is contained in the normal subgroup H. The stabilizer of ψ under this action is the centralizer G from the assertion. So we may bound

$$\#G \ge [\mathbf{Q}(E[N]) : \mathbf{Q}]/\#H \ge p^{-4}[\mathbf{Q}(E[N]) : \mathbf{Q}] \tag{5.7}$$

using (5.6).

Restricting $|\cdot|_p$ determines a place v of $\mathbf{Q}(E[N])$ lying above p. The Galois group $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ acts transitively on all places of $\mathbf{Q}(E[N])$ lying above p and the total number of such places is

$$\frac{[\mathbf{Q}(E[N]) : \mathbf{Q}]}{d_v} = \frac{[\mathbf{Q}(E[N]) : \mathbf{Q}]}{[\mathbf{Q}_p(E[N]) : \mathbf{Q}_p]}.$$

So the orbit Gv of v under the action of the group G has cardinality

$$\#Gv \ge \frac{1}{[\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}) : G]}\frac{[\mathbf{Q}(E[N]) : \mathbf{Q}]}{d_v} \ge \frac{1}{p^4}\frac{[\mathbf{Q}(E[N]) : \mathbf{Q}]}{d_v}.$$

by (5.7). □

At first we will only get a weak height inequality which holds for algebraic numbers satisfying a stronger condition than in Theorem 1.

Lemma 5.3. *Let E and p satisfy (P1). We assume $p|N$ and let $n \ge 1$ be the greatest integer with $p^n|N$. If $\alpha \in \mathbf{Q}(E[N])$ satisfies $\alpha^{Q(n)} \notin \mathbf{Q}_q(E[N/p])$, there exists a non-zero $\beta \in \overline{\mathbf{Q}} \smallsetminus \mu_\infty$ with $h(\beta) \le 2p^4 h(\alpha)$ and*

$$h(\alpha) + \max\left\{0, \frac{1}{[\mathbf{Q}(\beta) : \mathbf{Q}]}\sum_\tau \log|\tau(\beta) - 1|\right\} \ge \frac{\log p}{2p^8} \tag{5.8}$$

where the sum runs over all field embeddings $\tau : \mathbf{Q}(\beta) \to \mathbf{C}$.

Proof. For brevity, we set $Q = Q(n)$. By hypothesis we may choose $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$ with $\psi(\alpha^Q) \ne \alpha^Q$. We note that $\alpha \ne 0$.

We define

$$x = \psi(\alpha^Q) - \alpha^Q \in \mathbf{Q}(E[N])$$

and observe $x \ne 0$ by our choice of ψ. So

$$\sum_w d_w \log|x|_w = 0 \tag{5.9}$$

by the product formula.

Say G and v are as in Lemma 5.2. Let $\sigma \in G$. The place σv of $\mathbf{Q}(E[N])$ satisfies $|\sigma(y)|_{\sigma v} = |y|_v$ for all $y \in \mathbf{Q}(E[N])$. So $|(\sigma\psi\sigma^{-1})(\alpha^Q) - \alpha^Q|_{\sigma v} = |\psi(\sigma^{-1}(\alpha)^Q) - \sigma^{-1}(\alpha)^Q|_p$. By definition we have $q|Q$, so we may apply Lemma 4.2 to $\sigma^{-1}(\alpha)^{Q/q}$. This yields

$$\begin{aligned}|(\sigma\psi\sigma^{-1})(\alpha^Q) - \alpha^Q|_{\sigma v} &\leq p^{-1}\max\{1, |\psi(\sigma^{-1}(\alpha))|_p\}^Q \max\{1, |\sigma^{-1}(\alpha)|_p\}^Q \\ &\leq p^{-1}\max\{1, |(\sigma\psi\sigma^{-1})(\alpha))|_{\sigma v}\}^Q \max\{1, |\alpha|_{\sigma v}\}^Q\end{aligned}$$

Now $\sigma\psi\sigma^{-1} = \psi$ since $\sigma \in G$. Therefore,

$$|x|_w \leq p^{-1}\max\{1, |\psi(\alpha)|_w\}^Q \max\{1, |\alpha|_w\}^Q \quad \text{for all} \quad w \in Gv. \tag{5.10}$$

If w is an arbitrary finite place of $\mathbf{Q}(E[N])$, the ultrametric triangle inequality implies

$$|x|_w \leq \max\{1, |\psi(\alpha)|_w\}^Q \max\{1, |\alpha|_w\}^Q. \tag{5.11}$$

Say w is an infinite place. Applying the triangle inequality as for example in (5.4) to bound $|x|_w$ would lead to a ruinous factor 2. Instead we define

$$\beta = \frac{\psi(\alpha^Q)}{\alpha^Q} \in \overline{\mathbf{Q}} \smallsetminus \{1\}$$

and content ourselves by bounding

$$|x|_w = |\beta - 1|_w \, |\alpha|_w^Q \leq |\beta - 1|_w \max\{1, |\alpha|_w\}^Q. \tag{5.12}$$

We split the sum (5.9) up into the finite places in Gv, the remaining finite places, and the infinite places. The estimates (5.10), (5.11), and (5.12) together with the product formula (5.9) yield

$$\begin{aligned}0 \leq &\sum_{w \in Gv} d_w \log(p^{-1}) \\ &+ \sum_{w \nmid \infty} d_w Q \log(\max\{1, |\psi(\alpha)|_w\} \max\{1, |\alpha|_w\}) \\ &+ \sum_{w | \infty} d_w \left(\log|\beta - 1|_w + Q\log\max\{1, |\alpha|_w\}\right).\end{aligned} \tag{5.13}$$

Moreover, all local degrees d_w with $w \in Gv$ equal d_v. So the sum $\sum_{w \in Gv} d_w \log(p^{-1})$ is at most $-[\mathbf{Q}(E[N]) : \mathbf{Q}](\log p)/p^4$ by Lemma 5.2. We use this estimate together with (5.5) and (5.13) to obtain

$$0 \leq -\frac{\log p}{p^4} + \frac{1}{[\mathbf{Q}(E[N]) : \mathbf{Q}]}\left(\sum_{w|\infty} d_w \log|\beta - 1|_w\right) + Qh(\psi(\alpha)) + Qh(\alpha)$$

after dividing by $[\mathbf{Q}(E[N]) : \mathbf{Q}]$. The normalized sum over the infinite places is the normalized sum over the field embeddings found in (5.8).

Inequality (5.8) follows from $h(\psi(\alpha)) = h(\alpha)$ and $Q \leq p^4$. Basic height properties yield $h(\beta) \leq h(\psi(\alpha^Q)) + h(\alpha^Q) \leq 2Qh(\alpha) \leq 2p^4 h(\alpha)$.

By construction we certainly have $\beta \neq 0$ and it remains to show that β is not a root of unity. If we assume the contrary, then $\psi(\alpha)/\alpha$ is a root of unity too. Lemma 3.5(ii) implies $(\psi(\alpha)/\alpha)^Q = 1$, but this contradicts the choice of ψ. □

6. Descending Along p^n-Torsion

Let E be an elliptic curve defined over $\mathbf{Q}$ and let $p \geq 5$ be a prime with $q = p^2$.

Lemma 6.2 below is our main tool in the descent argument. Given an element in $\mathbf{Q}(E[p^nM])$ it allows us to decrease n under certain circumstances and work in the smaller field $\mathbf{Q}(E[p^{n-1}M])$. The proof involves the group theory of $\mathrm{GL}_2(\mathbf{F}_p)$. We thus begin by recalling some facts and proving a technical lemma.

The multiplicative group of an $\mathbf{F}_p$-subalgebra of $\mathrm{Mat}_2(\mathbf{F}_p)$ which is a field of cardinality q is called a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$. A non-split Cartan subgroup is cyclic of order $q-1$.

Conversely, if $G \subset \mathrm{GL}_2(\mathbf{F}_p)$ is a cyclic subgroup of order $q-1$, then it is a non-split Cartan subgroup. Indeed, if θ is a generator, then the Theorem of Cayley-Hamilton implies that G is contained in the commutative $\mathbf{F}_p$-subalgebra $\mathbf{F}_p + \mathbf{F}_p\theta \subset \mathrm{Mat}_2(\mathbf{F}_p)$; here $\mathbf{F}_p$ also denote the scalar matrices. Counting elements yields $G = (\mathbf{F}_p + \mathbf{F}_p\theta) \smallsetminus \{0\}$ and hence G is a non-split Cartan subgroup.

Lemma 6.1. *Let G be a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$. The set*

$$\{hgh^{-1};\ g \in G \text{ and } h \in \mathrm{GL}_2(\mathbf{F}_p)\}. \tag{6.1}$$

has cardinality strictly greater than p^3 and generates $\mathrm{GL}_2(\mathbf{F}_p)$ as a group.

Proof. The normalizer of G has cardinality $2(q-1)$ by Section 2.2 [16]. Therefore, the orbit of G under the action of $\mathrm{GL}_2(\mathbf{F}_p)$ by conjugation has cardinality at least $\#\mathrm{GL}_2(\mathbf{F}_p)/(2(q-1))$. Conjugating G by an element of $\mathrm{GL}_2(\mathbf{F}_p)$ gives again a non-split Cartan subgroup. If G' is a conjugate distinct from G, then $0 \cup (G \cap G')$ is an $\mathbf{F}_p$-subalgebra of $\{0\} \cup G$ and $\{0\} \cup G'$ that has cardinality strictly less than q. So $\{0\} \cup (G \cap G')$ has cardinality p since it contains the scalar matrices.

The set (6.1) equals the union of all elements in the orbit of G. Each orbit element contributes at least $q-p$ elements. So the cardinality of (6.1) is at least

$$\frac{q-p}{2(q-1)}\#\mathrm{GL}_2(\mathbf{F}_p) = \frac{(p-1)^2p^2}{2} > p^3 \tag{6.2}$$

since $p \geq 5$.

The subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$ generated by (6.1) contains the non-split Cartan subgroup G. By Serre's Proposition 17 [16] it is either $\mathrm{GL}_2(\mathbf{F}_p)$ or has cardinality at most $p(p-1)^2$. But the second alternative is impossible because of (6.2). □

Lemma 6.2. *Let E and p satisfy (P1) and (P2). We assume $N \in \mathbf{N}$ and $p|N$. If $\alpha \in \mathbf{Q}(E[N])$ with $\sigma(\alpha) \in \mathbf{Q}_q(E[N/p])$ for all $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$, then $\alpha \in \mathbf{Q}(E[N/p])$.*

Proof. Let α be as in the hypothesis. So all of its conjugates over $\mathbf{Q}$ lie in $\mathbf{Q}_q(E[N/p])$. We write $N = p^nM$ with $M, n \in \mathbf{N}$ and $p \nmid M$.

It is convenient to fix isomorphisms $E[p] \cong (\mathbf{Z}/p\mathbf{Z})^2$ and $E[p^n] \cong (\mathbf{Z}/p^n\mathbf{Z})^2$ that are compatible with the natural inclusion $E[p] \subset E[p^n]$. We will identify $\mathrm{Aut}\,E[p]$ and $\mathrm{Aut}\,E[p^n]$ with $\mathrm{GL}_2(\mathbf{F}_p)$ and $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$, respectively. There are two natural Galois representations

$$\widetilde{\rho} : \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p) \quad \text{and} \quad \rho : \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}).$$

The diagram

$$\begin{tikzcd}
\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}) \arrow[r] \arrow[d] \arrow[dr, "\widetilde{\rho}"'] & \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}) \arrow[d] \\
\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \arrow[r] & \mathrm{GL}_2(\mathbf{F}_p)
\end{tikzcd} \tag{6.3}$$

commutes; here the vertical arrows are the natural surjections, the left one is induced by the restriction map.

We introduce the group

$$G = \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p])).$$

and

$$H = \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])(\alpha)).$$

We recall the convention made in Section 2.2 and identify $\mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q)$ with a subgroup of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$. The hypothesis on α implies

$$\sigma\psi\sigma^{-1} \in H \quad \text{for all} \quad \sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}) \quad \text{and} \quad \psi \in G. \tag{6.4}$$

Let us now split up into two cases.

First we assume $n = 1$. Then G and $\mathrm{Gal}(\mathbf{Q}_q(E[p])/\mathbf{Q}_q)$ are isomorphic groups by Lemma 3.3(iii). Lemma 3.2(i) tells us that G is cyclic of order $q-1$. So is $\rho(G)$ because $\rho|_G$ is injective. Therefore, $\rho(G)$ is a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$.

By property (P1) the image of $\rho = \widetilde{\rho}$ is $\mathrm{GL}_2(\mathbf{F}_p)$. Its cardinality is $(p^2-1)(p^2-p) > 2(p-1)^2(p+1)$ since $p \geq 5$. So we may apply Lemma 6.1 to $\rho(G) \subset \mathrm{GL}_2(\mathbf{F}_p)$ to obtain

$$\rho(H) = \mathrm{GL}_2(\mathbf{F}_p). \tag{6.5}$$

The restriction map induces an injective homomorphism

$$\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])) \hookrightarrow \mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}).$$

In particular, we get the second inequality in

$$\#H \leq \#\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])) \leq \#\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}). \tag{6.6}$$

the first one follows from the definition of H. But $\#H \geq \#\mathrm{GL}_2(\mathbf{F}_p)$ by (6.5) and thus $\#H \geq \mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q})$. The chain of inequalities (6.6) is actually a chain of equalities. This implies $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])(\alpha)) = H = \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p]))$ and hence $\alpha \in \mathbf{Q}(E[N/p])$, as desired.

Now we treat the second case $n \geq 2$.

If $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p]))$ then $\rho(\sigma)$ is represented by $1 + p^{n-1}\mathcal{L}'(\sigma)$ with $\mathcal{L}'(\sigma) \in \mathrm{Mat}_2(\mathbf{Z})$. Moreover, $\mathcal{L}'(\sigma)$ is well-defined modulo $p\mathrm{Mat}_2(\mathbf{Z})$. We obtain a "logarithm" $\mathcal{L} : \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])) \to \mathrm{Mat}_2(\mathbf{F}_p)$. The name is justified since if $\sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p]))$, then

$$\rho(\sigma_1\sigma_2) \equiv (1 + p^{n-1}\mathcal{L}(\sigma_1))(1 + p^{n-1}\mathcal{L}(\sigma_2)) \equiv 1 + p^{n-1}(\mathcal{L}(\sigma_1) + \mathcal{L}(\sigma_2)) \mod p^n\mathrm{Mat}_2(\mathbf{Z})$$

because $n \geq 2$. So $\mathcal{L}(\sigma_1\sigma_2) = \mathcal{L}(\sigma_1) + \mathcal{L}(\sigma_2)$. Clearly, $\mathcal{L}$ is injective and we find

$$[\mathbf{Q}(E[N]) : \mathbf{Q}(E[N/p])] \leq \#\mathrm{Mat}_2(\mathbf{F}_p) = p^4. \tag{6.7}$$

If $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ and $\psi \in G$ then $\sigma\psi\sigma^{-1} \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p]))$ and a short calculation gives

$$\rho(\sigma\psi\sigma^{-1}) \equiv 1 + p^{n-1}\widetilde{\rho}(\sigma)\mathcal{L}'(\psi)\widetilde{\rho}(\sigma)^{-1} \mod p^n\mathrm{Mat}_2(\mathbf{Z}).$$

So

$$\mathcal{L}(\sigma\psi\sigma^{-1}) = \widetilde{\rho}(\sigma)\mathcal{L}(\psi)\widetilde{\rho}(\sigma)^{-1}. \tag{6.8}$$

The extension $\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q(E[p^{n-1}])$ is totally ramified and $\mathbf{Q}_q(E[N/p])/\mathbf{Q}_q(E[p^{n-1}])$ is unramified, cf. Lemma 3.3. By Lemma 2.1(i) restriction induces an isomorphism $G \cong \mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q(E[p^{n-1}]))$. So G has order p^2 by Lemma 3.2(i). We conclude $\#\mathcal{L}(G) = p^2$. In particular, $\mathcal{L}(G)$ contains a non-scalar matrix θ. One consequence of Lubin-Tate theory, cf. Lemma 3.2(iii), is that $\rho(G)$ contains all scalar matrices in $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Tracing through the definition of $\mathcal{L}$ this implies that $\mathcal{L}(G)$ contains the scalar matrices $\mathbf{F}_p \subset \mathrm{Mat}_2(\mathbf{F}_p)$. We have proved $\mathcal{L}(G) = \mathbf{F}_p + \mathbf{F}_p\theta$ and by the Theorem of Cayley-Hamilton $\mathcal{L}(G)$ is a commutative $\mathbf{F}_p$-algebra.

Next we claim that θ has no eigenvalues in $\mathbf{F}_p$. The group $\mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q)$ is abelian by Lemma 3.2(i) and it is isomorphic to $\mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[M]))$ by Lemma 3.3(iii). But (6.8) implies that $\widetilde{\rho}(\mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[M])))$ is inside the centralizer of θ. On the other hand, $\widetilde{\rho}(\mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[M])))$ is the image of $\mathrm{Gal}(\mathbf{Q}_q(E[p])/\mathbf{Q}_q)$ under the bottom arrow of (6.3). This arrow is injective and we know from Lemma 3.2(i) that $\mathrm{Gal}(\mathbf{Q}_q(E[p])/\mathbf{Q}_q)$ has order $q-1$. So $q-1$ divides the order of the centralizer of θ. Now if θ were to have an eigenvalue in $\mathbf{F}_p$ then it would be conjugate to either

$$\left(\begin{array}{cc} \phi & 0 \\ 0 & \mu \end{array}\right) \quad \text{or} \quad \left(\begin{array}{cc} \phi & 1 \\ 0 & \phi \end{array}\right)$$

with $\phi, \mu \in \mathbf{F}_p$. The only matrices listed above having centralizer of order divisible by $q-1$ are the scalar matrices. This contradicts our choice of θ.

Since θ has no eigenvalues in $\mathbf{F}_p$ we deduce $\mathcal{L}(G)^\times = \mathcal{L}(G) \smallsetminus \{0\}$. Hence $\mathcal{L}(G)$ is a field with q elements and $\mathcal{L}(G)^\times$ is a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$.

We recall that by (P2) the image of $\widetilde{\rho}$ is $\mathrm{GL}_2(\mathbf{F}_p)$. So (6.4) and (6.8) imply that conjugating a matrix in $\mathcal{L}(G)$ by any element of $\mathrm{GL}_2(\mathbf{F}_p)$ stays within $\mathcal{L}(H)$. We apply Lemma 6.1 to the subgroup $\mathcal{L}(G)^\times$ and deduce $\#\mathcal{L}(H) > p^3$. But $\mathcal{L}(H)$ is a subgroup of $\mathrm{Mat}_2(\mathbf{F}_2)$. So its cardinality must be p^4.

The conclusion of the case $n \geq 2$ is also similar to $n = 1$: we have

$$\#H = \#\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])(\alpha)) \leq \#\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])) \leq p^4 \tag{6.9}$$

where we also used (6.7). But $\#H \geq \#\mathcal{L}(H) = p^4$. This implies equality throughout (6.9). In other words $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])) = \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q}(E[N/p])(\alpha))$ which gives $\alpha \in \mathbf{Q}(E[N/p])$. □

Using this last lemma we can strengthen Lemma 5.3 to cover the tamely ramified case, i.e. for algebraic numbers in $\mathbf{Q}(E[N])$ when $p^2 \nmid N$.

Lemma 6.3. *Let E and p satisfy (P1) and (P2). We assume $N \in \mathbf{N}$ with $p^2 \nmid N$. If $\alpha \in \mathbf{Q}(E[N]) \smallsetminus \mu_\infty$ is non-zero, there exists a non-zero $\beta \in \overline{\mathbf{Q}} \smallsetminus \mu_\infty$ with $h(\beta) \leq 2p^4 h(\alpha)$ and*

$$h(\alpha) + \max\left\{0, \frac{1}{[\mathbf{Q}(\beta):\mathbf{Q}]}\sum_\tau \log|\tau(\beta) - 1|\right\} \geq \frac{\log p}{2p^8}$$

where the sum runs over all field embeddings $\tau : \mathbf{Q}(\beta) \to \mathbf{C}$.

Proof. For brevity we write $Q = Q(1) = (q-1)q$. It is no restriction to assume $p|N$. If there is $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ with $\sigma(\alpha)^Q \notin \mathbf{Q}_q(E[N/p])$ then we may apply Lemma 5.3 to $\sigma(\alpha)$. The current lemma follows because $h(\sigma(\alpha)) = h(\alpha)$.

Conversely, if $\sigma(\alpha^Q) \in \mathbf{Q}_q(E[N/p])$ for all σ, then Lemma 6.2 implies $\alpha^Q \in \mathbf{Q}(E[N/p])$.

But N/p and p are coprime by hypothesis. We can refer to the unramified case treated in Lemma 5.1 to deal with α^Q. Clearly α^Q is non-zero and not a root of unity. So

$$h(\alpha^Q) \geq \frac{\log(p/2)}{p^2+1}.$$

Basic height properties imply $h(\alpha^Q) = Qh(\alpha) = (p^2-1)p^2 h(\alpha)$, hence

$$h(\alpha) \geq \frac{\log(p/2)}{p^2(p^4-1)} \geq \frac{\log(p/2)}{p^6}.$$

This lower bound is better than $(\log p)/(2p^8)$ since $p \geq 5$. The current lemma follows with $\beta = \alpha$. □

Now we will find a useful automorphism of $\mathbf{Q}(E[N])/\mathbf{Q}$.

Lemma 6.4. *Let E and p satisfy (P1). We assume $N \in \mathbf{N}$ and let $n \geq 0$ be the greatest integer with $p^n|N$. There exists $\sigma \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q)$, lying in the center of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$, such that $\sigma(\zeta) = \zeta^4$ for all $\zeta \in \mu_{p^n}$. Moreover, σ acts on $E[p^n]$ as multiplication by 2.*

Before we prove this lemma, let us recall that $\mathbf{Q}_q(E[N])$ contains μ_{p^n} by Lemma 3.4.

Proof. Since p is odd, Lemma 3.2(iii) implies that there is $\sigma' \in \mathrm{Gal}(\mathbf{Q}_q(E[p^n])/\mathbf{Q}_q)$ which acts on $E[p^n]$ as multiplication by 2.

By properties of the Weil pairing we see that σ' acts as $\zeta \mapsto \zeta^4$ on the roots of unity of order dividing p^n; bilinearity of the Weil pairing is responsible for $4 = 2^2$ in the exponent.

By Lemma 3.3(iii) the automorphism σ' lifts uniquely to $\sigma \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[M]))$.

Taking the sum of points gives an isomorphism between $E[p^n] \times E[M]$ and $E[N]$ which is compatible with the action of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$. Since σ acts on $E[p^n]$ as multiplication by 2 and trivially on $E[M]$, it must lie in the center of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$. □

In the next proposition we fix the auxiliary prime p which has accompanied us until now. Its proof contains an Kummerian descent reminiscent to one used by Amoroso and Zannier [3].

Proposition 1. *Suppose E does not have complex multiplication. There exists a constant $c > 0$ depending only on E with the following property. If $\alpha \in \mathbf{Q}(E_{\mathrm{tors}}) \smallsetminus \mu_\infty$ is non-zero, there is a non-zero $\beta \in \overline{\mathbf{Q}} \smallsetminus \mu_\infty$ with $h(\beta) \leq c^{-1}h(\alpha)$ and*

$$h(\alpha) + \max\left\{0, \frac{1}{[\mathbf{Q}(\beta):\mathbf{Q}]} \sum_{\tau:\mathbf{Q}(\beta)\to\mathbf{C}} \log|\tau(\beta)-1|\right\} \geq c. \tag{6.10}$$

Proof. Since E does not have complex multiplication, its j-invariant is not 0 or 1728. So the reduction of E at p is an elliptic curve with j-invariant not among $\{0, 1728\}$ for all but finitely many primes p. By a theorem of Serre [16] all but finitely many of these p satisfy (P2), that is, the representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. By Elkies' Theorem [11], E has good supersingular reduction at infinitely many primes. We may thus fix a prime $p \geq 5$ satisfying both (P1) and (P2).

Let α be as in the hypothesis. We fix $N \in \mathbf{N}$ with $\alpha \in \mathbf{Q}(E[N])$ and write $N = p^n M$ with $M \in \mathbf{N}$ coprime to p and $n \geq 0$.

We take $\sigma_4 \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q)$ as in Lemma 6.4. So σ_4 lies in the center of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ and $\sigma_4(\zeta) = \zeta^4$ for $\zeta \in \mu_{p^n}$.

We define

$$\gamma = \frac{\sigma_4(\alpha)}{\alpha^4} \in \mathbf{Q}(E[N]) \smallsetminus \{0\}. \tag{6.11}$$

Basic height inequalities imply

$$h(\gamma) \leq h(\sigma_4(\alpha)) + h(\alpha^4) = 5h(\alpha). \tag{6.12}$$

There is a least integer $n' \geq 0$ such that $\sigma(\gamma) \in \mathbf{Q}_q(E[p^{n'}M])$ for all $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$. It satisfies $n' \leq n$ and Lemma 6.2 implies $\gamma \in \mathbf{Q}(E[p^{n'}M])$.

Let us first suppose $n' \leq 1$, so $\gamma \in \mathbf{Q}(E[pM])$. We want to apply Lemma 6.3, so let us confirm that γ is not a root of unity. Otherwise we would have $4h(\alpha) = h(\alpha^4) = h(\gamma\alpha^4) = h(\sigma_4(\alpha)) = h(\alpha)$ by the basic height properties. So $h(\alpha) = 0$. Kronecker's Theorem implies $\alpha = 0$ or $\alpha \in \mu_\infty$. This contradicts our assumption on α. Hence Lemma 6.3 provides a non-zero $t \in \overline{\mathbf{Q}} \smallsetminus \mu_\infty$ with $h(\beta) \leq 2p^4 h(\gamma)$. The bound (6.12) gives $h(\beta) \leq 10p^4 h(\alpha)$. Moreover, we can use (6.12) again to deduce (6.10) with a constant c depending only on p.

Hence Proposition 1 follows if $n' \leq 1$ and we will now assume $n' \geq 2$.

By minimality of n' there is $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ with $\sigma(\gamma) \notin \mathbf{Q}_q(E[p^{n'-1}M])$. We abbreviate $\alpha' = \sigma(\alpha)$ and $\gamma' = \sigma(\gamma)$. We apply σ to (6.11) and obtain

$$\gamma' = \frac{\sigma(\sigma_4(\alpha))}{\sigma(\alpha)^4} = \frac{\sigma_4(\sigma(\alpha))}{\sigma(\alpha)^4} = \frac{\sigma_4(\alpha')}{\alpha'^4} \tag{6.13}$$

since σ_4 lies in the center of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$.

Next we would like to apply Lemma 5.3 to γ'. In order to do this we need to verify the hypotheses. Note that we have $Q(n') = q$ since $n' \geq 2$, so we must prove $\gamma'^q \notin \mathbf{Q}_q(E[p^{n'-1}M])$. We now assume the contrary and will soon arrive at a contradiction.

Since $\gamma' \notin \mathbf{Q}_q(E[p^{n'-1}M])$ there is $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[p^{n'-1}M]))$ with $\psi(\gamma') \neq \gamma'$. However, $\psi(\gamma'^q) = \gamma'^q$ and so

$$\psi(\gamma') = \xi\gamma' \quad \text{with} \quad \xi^q = 1 \quad \text{while} \quad \xi \neq 1. \tag{6.14}$$

We identify ψ with its restriction to $\mathbf{Q}(E[N])$, apply (6.13) and obtain

$$\xi\gamma' = \frac{\sigma_4(\psi(\alpha'))}{\psi(\alpha')^4}$$

having used that ψ commutes with σ_4. We define $\eta = \psi(\alpha')/\alpha' \neq 0$ and get

$$\xi = \frac{\sigma_4(\eta)}{\eta^4}.$$

Basic height properties and the fact that ξ is a root of unity give $4h(\eta) = h(\eta^4) = h(\xi\eta^4) = h(\sigma_4(\eta)) = h(\eta)$. As usual, we conclude $h(\eta) = 0$. So η is a root of unity by Kronecker's Theorem.

We have just shown $\psi(\alpha')/\alpha' \in \mu_\infty$. We fix $\widetilde{M} \in \mathbf{N}$ coprime to p such that $(\psi(\alpha')/\alpha')^{\widetilde{M}} \in \mu_{p^\infty}$. Lemma 3.4 implies $(\psi(\alpha')/\alpha')^{\widetilde{M}} \in \mu_{p^n}$. So σ_4 raises this element to the fourth power, hence

$$\sigma_4\left(\frac{\psi(\alpha')}{\alpha'}\right) = \xi'\left(\frac{\psi(\alpha')}{\alpha'}\right)^4$$

with $\xi'^{\widetilde{M}} = 1$. We rearrange this expression to obtain

$$\frac{\sigma_4(\psi(\alpha'))}{\psi(\alpha')^4} = \xi'\frac{\sigma_4(\alpha')}{\alpha'^4} = \xi'\gamma'$$

using (6.13). Applying again the fact that ψ and σ_4 commute gives

$$\psi(\gamma') = \frac{\psi(\sigma_4(\alpha'))}{\psi(\alpha')^4} = \frac{\sigma_4(\psi(\alpha'))}{\psi(\alpha')^4} = \xi'\gamma'.$$

We recall (6.14) and find $\xi' = \xi$, so $\xi^{\widetilde{M}} = \xi^q = 1$. But $\widetilde{M}$ and $q = p^2$ are coprime, hence $\xi = 1$. This contradicts (6.14).

So we must have $\gamma'^q \notin \mathbf{Q}_q(E[p^{n'-1}M])$ and Lemma 5.3 yields

$$h(\gamma') + \max\left\{0, \frac{1}{[\mathbf{Q}(\beta):\mathbf{Q}]}\sum_\tau \log|\tau(\beta) - 1|\right\} \geq \frac{\log p}{2p^8}$$

for some non-zero $\beta \in \mathbf{Q}(E[N]) \smallsetminus \mu_\infty$ satisfying $h(\beta) \leq 2p^4 h(\gamma')$. We have $h(\gamma') = h(\gamma) \leq 5h(\alpha)$ by (6.12) so

$$h(\beta) \leq 10p^4 h(\alpha).$$

We may also bound

$$h(\alpha) + \max\left\{0, \frac{1}{[\mathbf{Q}(\beta):\mathbf{Q}]}\sum_\tau \log|\tau(\beta) - 1|\right\} \geq \frac{\log p}{10p^8}.$$

The proof follows after choosing c appropriately. □

7. Equidistribution

After an extensive analysis on the places above a fixed prime p we turn our attention to the infinite places.

Let us suppose for the moment that we are in the situation of the Proposition 1. The normalized sum over τ is by definition of the height at most $h(\beta - 1)$. So the bound (6.10) entails

$$h(\alpha) + h(\beta - 1) \geq c.$$

Basic height inequalities show

$$h(\beta - 1) \leq h(\beta) + \log 2.$$

Indeed, $\log 2$ originates from the triangle inequality

$$\log|\beta - 1|_v \leq \log(|\beta|_v + 1) \leq \log\max\{1, |\beta|_v\} + \log 2$$

which holds for any infinite place v of the number field $\mathbf{Q}(\beta)$. Our proposition also implies $h(\beta) \le c^{-1}h(\alpha)$, so β has small height if α does. We find

$$(1+c^{-1})h(\alpha) + \log 2 \ge c.$$

Unfortunately, $\log 2$ spoils the inequality completely; we obtain no information on $h(\alpha)$.

What we need is a more refined estimate involving the infinite places. This is provided by Bilu's Equidistribution Theorem [6] which takes into account that β has small height. We state it in a form streamlined for our application.

Theorem 3 (Bilu)**.** *Let $\beta_1, \beta_2, \ldots$ be a sequence of non-zero elements of $\overline{\mathbf{Q}} \smallsetminus \mu_\infty$ with $\lim_{k\to\infty} h(\beta_k) = 0$. If $f : \mathbf{C} \smallsetminus \{0\} \to \mathbf{R}$ is a continuous and bounded function, then*

$$\lim_{k\to\infty} \frac{1}{[\mathbf{Q}(\beta_k):\mathbf{Q}]} \sum_{\tau} f(\tau(\beta_k)) = \int_0^1 f(e^{2\pi i t})dt$$

where τ runs over all field embeddings $\mathbf{Q}(\beta_k) \to \mathbf{C}$.

We now prove Theorem 1.

If E has complex multiplication with endomorphisms defined over a number field K, then $K(E_{\mathrm{tors}})$ is an abelian extension of K. By the result of Amoroso and Zannier [2] the field $K(E_{\mathrm{tors}})$ satisfies the Bogomolov property. Hence so does its subfield $\mathbf{Q}(E_{\mathrm{tors}})$ and this yields the desired result.

So let us assume that E does not have complex multiplication.

Our argument is by contradiction. We suppose that $\alpha_1, \alpha_2, \ldots$ is a sequence of non-zero elements of $\mathbf{Q}(E_{\mathrm{tors}}) \smallsetminus \mu_\infty$ with $\lim_{k\to\infty} h(\alpha_k) = 0$.

Let $m \in \mathbf{N}$ we define a continuous and bounded function $f_m : \mathbf{C} \smallsetminus \{0\} \to \mathbf{R}$ by setting

$$f_m(z) = \min\{m, \max\{-m, \log|z-1|\}\}$$

for $z \ne 1$ and $f_m(1) = -m$.

The sequence of functions $s \mapsto f_m(e^{2\pi i s})$ converges pointwise to $s \mapsto \log|e^{2\pi i s} - 1|$ on $(0,1)$ as $m \to \infty$. Clearly, $|f_m(e^{2\pi i s})| \le |\log|e^{2\pi i s}-1||$ and $\int_0^1 |\log|e^{2\pi i s}-1||ds < \infty$. So the Dominant Convergence Theorem from analysis implies

$$\lim_{m\to\infty} \int_0^1 f_m(e^{2\pi i s})ds = \int_0^1 \log|e^{2\pi i s}-1|ds.$$

The latter integral is the logarithmic Mahler measure of the polynomial $X-1$. As such, it vanishes by Jensen's Formula. So we may fix once and for all an m such that

$$\int_0^1 f(e^{2\pi i s})ds < \frac{c}{2} \quad \text{and} \quad \log(1+2e^{-m}) \le \frac{c}{2} \tag{7.1}$$

where c is the positive constant from Proposition 1 and $f = f_m$.

The proposition also gives us a non-zero $\beta_k \in \overline{\mathbf{Q}} \smallsetminus \mu_\infty$ for each α_k which satisfies

$$h(\alpha_k) + \max\left\{0, \frac{1}{[\mathbf{Q}(\beta_k):\mathbf{Q}]} \sum_{\tau:\mathbf{Q}(\beta_k)\to\mathbf{C}} \log|\tau(\beta_k)-1|\right\} \ge c. \tag{7.2}$$

and

$$h(\beta_k) \le \frac{h(\alpha_k)}{c}. \tag{7.3}$$

We proceed by bounding the sum in (7.2) from above. Let $\tau : \mathbf{Q}(\beta_k) \to \mathbf{C}$ be an embedding. We write $z = \tau(\beta_k) \in \mathbf{C} \smallsetminus \{0, 1\}$ and split up into cases depending on the size of $|z - 1|$.

Suppose for the moment that $|z - 1| \geq e^m$. Then $|z| \geq e^m - 1 \geq e^m/2$ since $m \geq 1$. So $|z - 1|/|z| \leq 1 + 1/|z| \leq 1 + 2e^{-m}$. Applying the logarithm and using (7.1) gives

$$\log|z - 1| \leq \log(1 + 2e^{-m}) + \log|z| \leq \frac{c}{2} + \log|z| \leq \frac{c}{2} + \log\max\{1, |z|\}.$$

Because $f(z) = m \geq 0$ we conclude

$$\log|\tau(\beta_k) - 1| \leq \frac{c}{2} + \log\max\{1, |\tau(\beta_k)|\} + f(\tau(\beta_k)). \tag{7.4}$$

The second case is $|z - 1| < e^m$. Then $\log|z - 1| \leq \max\{-m, \log|z - 1|\} = f(z)$. So (7.4) holds as well.

Taking the sum over all field embeddings $\tau : \mathbf{Q}(\beta_k) \to \mathbf{C}$, applying (7.4), and dividing by the degree yields

$$\frac{1}{[\mathbf{Q}(\tau_k) : \mathbf{Q}]}\sum_{\tau} \log|\tau(\beta_k) - 1| \leq \frac{c}{2} + h(\beta_k) + \frac{1}{[\mathbf{Q}(\tau_k) : \mathbf{Q}]}\sum_{\tau} f(\tau(\beta_k)).$$

Hence (7.2) implies

$$h(\alpha_k) + \max\left\{0, \frac{c}{2} + h(\beta_k) + \frac{1}{[\mathbf{Q}(\tau_k) : \mathbf{Q}]}\sum_{\tau} f(\tau(\beta_k))\right\} \geq c. \tag{7.5}$$

The sequence $h(\alpha_1), h(\alpha_2), \ldots$ tends to zero, hence so does $h(\beta_1), h(\beta_2), \ldots$ by (7.3). We will apply Bilu's Theorem to $\beta_1, \beta_2, \ldots$ and the function f. On letting $k \to \infty$ the sum (7.5) over the τ converges to the integral $\int_0^1 f(e^{2\pi i s})ds < c/2$ and both terms involving the height vanish. This is a contradiction. □

8. Height Lower Bounds on Elliptic Curves

8.1. **The Néron-Tate Height.** Let E be an elliptic curve defined over a number field F. We suppose that E is presented by a short Weierstrass equation.

The Néron-Tate height takes a point $A \in E(F)$ to a real number $\hat{h}(A) \geq 0$. It can be defined either as a sum of local heights or a limit process involving the Weil height. We begin with a brief review of the first definition. Say v is a place of F and let E_v be E taken as an elliptic curve defined over F_v. When working at a fixed place we will assume $F \subset F_v$. There is a local height function $\lambda_v : E(F_v) \smallsetminus \{0\} \to \mathbf{R}$, some of whose properties are discussed below. These local height functions are defined in Chapter VI [17] and they are independent of the chosen Weierstrass equation. They sum up to give the Néron-Tate height

$$\hat{h}(A) = \frac{1}{[F : \mathbf{Q}]}\sum_{v \text{ place of } F} d_v\lambda_v(A)$$

for $A \neq 0$. We remark that only finitely many terms $\lambda_v(A)$ are non-zero and set $\hat{h}(0) = 0$. Let K be a number field containing F and w a place of K extending v. Then we may take $F_v \subset K_w$ and we have $\lambda_v = \lambda_w$ on $E(F_v)$. So we obtain a local height function $\lambda_v : E(\overline{F_v}) \smallsetminus \{0\} \to \mathbf{R}$ where $\overline{F_v}$ is an algebraic closure of F_v.

Because we are working with a Weierstrass equation any $A \in E(F) \smallsetminus \{0\}$ can be expressed as $A = (x, y)$. We set $h(A) = h(x)/2$ and $h(0) = 0$. The definition of the Néron-Tate height in terms of local heights is equivalent to

$$\hat{h}(A) = \lim_{k\to\infty} \frac{h([2^k](A))}{4^k}.$$

We refer to Chapter VIII, §9 [18] for the basic properties of the Néron-Tate height which follow.

The Néron-Tate height does not depend on the number field F over which the point A is defined. We thus obtain a well-defined function $\hat{h} : E(\overline{F}) \to [0, \infty)$ on any algebraic closure $\overline{F}$ of F. The elliptic version of Kronecker's Theorem also holds: the Néron-Tate height vanishes precisely on E_{tors}. Moreover, it satisfies the parallelogram equality

$$\hat{h}(A + B) + \hat{h}(A - B) = 2\hat{h}(A) + 2\hat{h}(B)$$

for all $A, B \in E(\overline{F})$ as well as

$$\hat{h}(nA) = n^2\hat{h}(A)$$

for all $n \in \mathbf{Z}$. A direct consequence is $\hat{h}(A + B) = \hat{h}(A)$ if B happens to be a torsion point.

If $\ell \geq 2$ is a prime number of $\ell = \infty$ it will be convenient to define the partial height function

$$\hat{h}_\ell(A) = \frac{1}{[F : \mathbf{Q}]} \sum_{v|\ell} d_v \lambda_v(A)$$

if $A \in E(F) \smallsetminus \{0\}$. Then $\hat{h}_\ell$ extends to a well-defined function $E(\overline{F}) \smallsetminus \{0\} \to \mathbf{R}$. In this notation

$$\hat{h} = \hat{h}_\infty + \hat{h}_2 + \hat{h}_3 + \cdots .$$

We briefly discuss some relevant equidistribution properties of local height functions. To do this let v be a place of F.

Suppose first that v is an infinite place of F. Up to complex conjugation, v determines a field embedding $\sigma_0 : F \to \mathbf{C}$. We thus obtain an elliptic curve E_v defined over $\mathbf{C}$. The local height function $\lambda_v : E_v(\mathbf{C}) \smallsetminus \{0\} \to \mathbf{R}$ is given explicitly in Theorem VI.3.2 [17]. There is $\tau \in \mathbf{C}$ with positive imaginary part $\mathrm{Im}(\tau)$ and a complex analytic isomorphism $\mathbf{C}/(\mathbf{Z}+\tau\mathbf{Z}) \to E_v(\mathbf{C})$ of groups involving the Weierstrass elliptic function. We abbreviate $q = e^{2\pi i\tau}$ and remark $|q| < 1$. If $A \in E_v(\mathbf{C}) \smallsetminus \{0\}$ is the image of $z \in \mathbf{C}$ and $u = e^{2\pi iz}$, then

$$\lambda_v(A) = -\frac{1}{2} b_2 \left(\frac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}\right) \log|q| - \log|1 - u| - \sum_{n\geq 1} \log|(1 - q^n u)(1 - q^n u^{-1})| \tag{8.1}$$

where $b_2 = X^2 - X + 1/6$ is the second Bernoulli polynomial.

The group $E_v(\mathbf{C})$ endowed with the complex topology is compact. Hence it comes with a unique Haar measure $\mu_{E,v}$ of total measure 1.

A sufficiently strong analog to Bilu's Equidistribution Theorem is given by Szpiro, Ullmo, and Zhang's Théorème 1.2 [20] which we state in simplified form.

Theorem 4 (Szpiro, Ullmo, Zhang)**.** *We keep the notation above. Let* $P_1, P_2, \ldots \in E(\overline{F}) \smallsetminus E_{\mathrm{tors}}$ *be a sequence of points with* $\lim_{k\to\infty} \hat{h}(P_k) = 0$. *If* $f : E_v(\mathbf{C}) \to \mathbf{R}$ *is a continuous function, then*

$$\lim_{k\to\infty} \frac{1}{[F(P_k):F]} \sum_{\sigma} f(\sigma(P_k)) = \int f\mu_{E,v}$$

where σ *runs over all field embeddings* $\sigma : F(P_k) \to \mathbf{C}$ *extending* σ_0.

Now suppose v is a finite place of F where E has good reduction. If $A = (x, y) \in E_v(F_v) \smallsetminus \{0\}$, we have

$$\lambda_v(A) = \frac{1}{2} \max\{0, \log|x|_v\} \tag{8.2}$$

by Theorem VI.4.1 [17]. In particular, $\lambda_v(A) \geq 0$.

Suppose E_v has split multiplicative reduction. The local height can be evaluated using the Tate uniformization. More precisely, there is $q \in F_v^\times$ with $|q|_v < 1$ and a surjective group homomorphism $\phi : F_v^\times \to E(F_v)$ with kernel $q^{\mathbf{Z}}$, the cyclic group generated by q. Thus any point $A \in E(F_v) \smallsetminus \{0\}$ is $\phi(u)$ for some $u \in F_v^\times \smallsetminus q^{\mathbf{Z}}$ with $|q|_v < |u|_v \leq 1$. By Theorem VI.4.2 [17] we have

$$\lambda_v(A) = -\frac{1}{2} b_2 \left(\frac{\log|u|_v}{\log|q|_v}\right) \log|q|_v - \log|1-u|_v, \tag{8.3}$$

the non-Archimedean analog of (8.1).

The Tate uniformization extends to a group homomorphism $\overline{F_v}^\times \to E_v(\overline{F_v})$ with Kernel $q^{\mathbf{Z}}$. The expression for $\lambda_v(A)$ above holds for all $A \in E(\overline{F_v}) \smallsetminus \{0\}$. It is evident that λ_v is invariant under the operation of $\mathrm{Gal}(\overline{F_v}/F_v)$.

The topological group $\mathbf{R}/\mathbf{Z}$ is homeomorphic to the unit circle and thus equipped with the unique Haar measure $\mu_{\mathbf{R}/\mathbf{Z}}$ of total mass 1. The preimage under ϕ of a point $A \in E_v(\overline{F_v})$ determines $\log|u|_v \in \mathbf{R}$ uniquely up to addition of an integral multiple of $\log|q|_v$. Hence the coset $\log|u|_v/\log|q|_v + \mathbf{Z}$ is a well-defined element $l_v(A) \in \mathbf{R}/\mathbf{Z}$.

Say $K \subset \overline{F_v}$ is a finite extension of F_v. Then $\mathrm{slog}\,|K^\times|/\log|q|_v + \mathbf{Z} \subset \mathbf{R}/\mathbf{Z}$ is in bijection with the irreducible components of the Néron model of E taken as an elliptic curve defined over K. Roughly speaking, the set of these irreducible components becomes the group of torsion points on $\mathbf{R}/\mathbf{Z}$ when K is replaced by the "limit" $\overline{F_v}$. Let $\overline{F}$ be the algebraic closure of F in $\overline{F_v}$. Chambert-Loir's Theorem implies that the reduction of the conjugates of a point in $E(\overline{F})$ of sufficiently small Néron-Tate height are sufficiently even distributed on these irreducible components. His result holds for abelian varieties. But we state it, according to our needs, for an elliptic curve.

Theorem 5 (Chambert-Loir, Corollaire 5.5 [9])**.** *We keep the notation above. Let* $P_1, P_2, \ldots \in E(\overline{F}) \smallsetminus E_{\mathrm{tors}}$ *be a sequence of points with* $\lim_{k\to\infty} \hat{h}(P_k) = 0$. *If* $f : \mathbf{R}/\mathbf{Z} \to \mathbf{R}$ *is a continuous function, then*

$$\lim_{k\to\infty} \frac{1}{[F(P_k):F]} \sum_{\sigma} f(l_v(\sigma(P_k))) = \int f\mu_{\mathbf{R}/\mathbf{Z}}$$

where σ *runs over all field embeddings* $F(P_k) \to \overline{F_v}$ *which are the identity on* F.

The cases when E_v has non-split multiplicative or additive reduction will not be relevant for our application.

8.2. **Proof of Theorem 2.** Let E be an elliptic curve defined over $\mathbf{Q}$. In the current section we prove that a non-torsion point with coordinates in $\mathbf{Q}(E_{\text{tors}})$ cannot have arbitrarily small Néron-Tate height. As already explained in the introduction, the method of proof is quite similar to the proof that $\mathbf{Q}(E_{\text{tors}})$ has the Bogomolov property. We proceed by proving a series of lemmas, most of which have counterparts in previous sections.

If p is any prime then $E[p^\infty] = \bigcup_{n\geq 0} E[p^n]$ denotes the subgroup of E_{tors} of elements with order a power of p.

We fix some notation used throughout this section. Let p be a prime which satisfies properties (P1) and (P2) with respect to E. We set $q = p^2$. Let N be a positive integer with $N = p^n M$ where $M \in \mathbf{N}$ is coprime to p and n is a non-negative integer. It will also be convenient to fix a short Weierstrass equation for E with integer coefficients which has good reduction at p.

Our first lemma is the analog to Lemma 3.4.

Lemma 8.1. *We have $E(\mathbf{Q}_q(E[N])) \cap E[p^\infty] = E[p^n]$.*

Proof. The inclusion "$\supset$" is obvious. So let $T \in E(\mathbf{Q}_q(E[N]))$ be a torsion point of order $p^{n'}$. Without loss of generality, we may assume $n' \geq n$ and $n' \geq 1$.

By Lemma 3.2(iii) the Galois group $\mathrm{Gal}(\mathbf{Q}_q(E[p^{n'}])/\mathbf{Q}_q)$ acts transitively on the torsion points of order $p^{n'}$. Now any conjugate of T over $\mathbf{Q}_q$ is again defined over $\mathbf{Q}_q(E[N])$. Hence we find $\mathbf{Q}_q(E[p^{n'}]) \subset \mathbf{Q}_q(E[N])$. By Lemmas 3.2 and 3.3 the ramification index of $\mathbf{Q}_q(E[p^{n'}])/\mathbf{Q}_q$ is $(q-1)q^{n'-1}$ and that of $\mathbf{Q}_q(E[N])/\mathbf{Q}_q$ is either 1 or $(q-1)q^{n-1}$, depending on whether $n = 0$ or $n \geq 1$. The first ramification index is at most the second one, so we deduce $n' \leq n$. □

The next lemma is the elliptic version of Lemma 3.5. We reuse the symbol $Q(n)$.

Lemma 8.2. *Let us suppose $n \geq 1$. If $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$ and $A \in E(\mathbf{Q}_q(E[N]))$ such that $\psi(A) - A \in E_{\text{tors}}$, then*

$$\psi(A) - A \in E[Q(n)].$$

Proof. The order of $\psi(A) - A$ is $N' = p^{n'}M'$ for some integers $n' \geq 0$ and $M' \geq 1$ with $p \nmid M'$. The point $T = \psi([M'](A)) - [M'](A)$ has order $p^{n'}$. Since it lies in $E(\mathbf{Q}_q(E[p^n M]))$ we have $n' \leq n$ by Lemma 8.1.

We set $K = \mathbf{Q}_q(E[p^n])$ and $L = \mathbf{Q}_q(E[MM'])$ and remark that KL/L is an abelian extension by Lemmas 2.1, 3.2, and 3.3. Furthermore, there is a unique lift of ψ to the abelian Galois group $\mathrm{Gal}(KL/L)$. We use the same symbol ψ for this lift.

Let $B = [p^{n'}](A)$, then $\psi(B) - B$ has order M'. The extension $(KL)^\psi(B)/(KL)^\psi$ is Galois. All points of order M' in E are already defined over $L \subset (KL)^\psi$. The Kummer map $\mathrm{Gal}((KL)^\psi(B)/(KL)^\psi) \to E[M']$ given by $\sigma \mapsto \sigma(B) - B$ is therefore an injective group homomorphism. But $\mathrm{Gal}((KL)^\psi(B)/(KL)^\psi)$ is generated by the restriction of ψ whose image in $E[M']$ has order M'. So $[(KL)^\psi(B) : (KL)^\psi] = M'$ which is coprime to p.

Let us suppose for the moment that $n \geq 2$. Then as in the proof of Lemma 3.5 we see that $\mathrm{Gal}(KL/\mathbf{Q}_q(E[p^{n-1}])L) \cong (\mathbf{Z}/p\mathbf{Z})^2$. But $[(KL)^\psi(B) : (KL)^\psi]$ must divide this quantity. By the previous paragraph we deduce $M' = 1$.

Now we suppose $n = 1$. As in the proof of Lemma 3.5 we find that $\mathrm{Gal}(KL/\mathbf{Q}_q(E[p^{n-1}])L)$ is cyclic of order $q-1$. This time we have $M'|q-1$.

To summarize: $\psi(A) - A$ has order $p^{n'}$ if $n \geq 2$ and $[q-1](\psi(A)-A)$ has order $p^{n'}$ if $n = 1$.

We recall that $Q(n) = q$ if $n \geq 2$ and $Q(1) = q(q-1)$. Hence we are done if $n' = 0$, so let us suppose $n' \geq 1$. Further up we showed $n' \leq n$, so $n \geq 1$ and $C = [Q(n)/p](A)$ makes sense as an element of $E(\mathbf{Q}_q(E[N]))$. Regardless of the value of n, the difference $\psi(C) - C$ has order $p^{n'-1}$. Thus $[p^{n'-1}](C) \in E((KL)^\psi)$. Now $(KL)^\psi \supset \mathbf{Q}_q(E[p^{n-1}])$. So the map $\sigma \mapsto \sigma(C) - C$ determines an injective homomorphism of groups $\mathrm{Gal}((KL)^\psi(C)/(KL)^\psi) \to E[p^{n'-1}]$. As before, the restriction of ψ generates $\mathrm{Gal}((KL)^\psi(C)/(KL)^\psi)$ and maps to an element of order $p^{n'-1}$. So $(KL)^\psi(C)/(KL)^\psi$ is cyclic of order $p^{n'-1}$. Its Galois group is a quotient of $\mathrm{Gal}(KL/(KL)^\psi)$ and this is a subgroup of $\mathrm{Gal}(KL/\mathbf{Q}_q(p^{n-1})L)$. We have already remarked that the latter group is either isomorphic to $(\mathbf{Z}/p\mathbf{Z})^2$ if $n \geq 2$ or $\mathbf{Z}/(q-1)\mathbf{Z}$ when $n = 1$. Elementary group theory implies $n' \leq 2$. So $[p](\psi(C) - C) = 0$ and this implies $[Q(n)](\psi(A) - A) = 0$. □

As usual we will take $\mathbf{Q}(E[N])$ as a subfield of $\mathbf{Q}_q(E[N])$. The absolute value $|\cdot|_p$ on $\mathbf{Q}_q(E[N])$ induces a place v of $\mathbf{Q}(E[N])$. We let $\widetilde{E}$ denote the reduction of E at p. We take it as an elliptic curve defined over $\mathbf{F}_q$. Let $a_q \in \mathbf{Z}$ be the trace of q-Frobenius as in Section 3. By Lemma 3.1 we have $a_q = \pm 2p$.

Next we must translate the two metric lemmas from Section 4.

The first variant deals with the unramified case. Recall that $\varphi_q \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_q)$ is a lift of the q-Frobenius. It acts on $E(\overline{\mathbf{Q}}_p)$ just as any element of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

Lemma 8.3. *If $p \nmid N$ and $A \in E(\mathbf{Q}_q(E[N]))$ with $\varphi_p(A) \neq [a_q/2](A)$, then*

$$\lambda_v(\varphi_q(A) - [a_q/2](A)) \geq \frac{1}{2}\log p.$$

Proof. By Lemma 3.1 $\widetilde{\varphi_q}$, the q-Frobenius endomorphism of $\widetilde{E}$ acts as multiplication by $a_q/2$ on the reduction. Therefore, $\varphi_q(A) - [a_q/2](A)$ reduces to 0. Since E has good reduction at v, we may use (8.2) to evaluate $\lambda_v(\varphi_q(A) - [a_q/2](A))$. The lemma follows since $\mathbf{Q}_q(E[N])/\mathbf{Q}_q$ is unramified by Lemma 3.3. □

The second variant deals with the ramified case.

Lemma 8.4. *If $p|N$ and $A \in E(\mathbf{Q}_q(E[N]))$, then*

$$\lambda_v(\psi(A) - A) \geq \frac{\log p}{2(p^2-1)} \tag{8.4}$$

for all $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$ with $\psi(A) \neq A$.

Proof. As in the proof of Lemma 4.2 we find that ψ lies in the higher ramification group $G_i(\mathbf{Q}_q(E[N])/\mathbf{Q}_q)$ with $i = q^{n-1} - 1$. Let $\mathfrak{P}$ be the maximal ideal of the ring of integers of $\mathbf{Q}_q(E[N])$. Then $\psi(A)$ and A map to same element on E reduced modulo $\mathfrak{P}^{q^{n-1}}$. Suppose x is the first coordinate of $\psi(A) - A$ in our fixed Weierstrass model of E. Then

$\log|x|_p \geq \frac{q^{n-1}}{e}\log p$ with e the ramification index of $\mathbf{Q}_q(E[N])/\mathbf{Q}_q$. By Lemmas 3.2 and 3.3 we have $e = (q-1)q^{n-1}$. Now (8.4) follows from (8.2) and $q = p^2$. □

According to the blueprint of Theorem 1's proof the next step should be to imitate Lemma 5.1 and obtain a height lower bound in the unramified case. We postpone this task until later and for now only obtain a lower bound for the partial height function $\hat{h}_p$. The Néron-Tate height is the sum of all partial height functions, but the partial height functions at primes of bad reduction or at ∞ may take negative values. So a lower bound for $\hat{h}_p$ does not directly imply a lower bound for $\hat{h}$.

Lemma 8.5. *We assume $p \nmid N$. If $A \in E(\mathbf{Q}(E[N])) \smallsetminus E_{\mathrm{tors}}$ there is a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with $\hat{h}(B) \leq 2(p^2+1)\hat{h}(A)$ such that*

$$\hat{h}_p(B) \geq \frac{1}{2}\log p.$$

Proof. We set $B = \varphi_q(A) - [a_q/2](A)$ and remark that B is not a torsion point. Indeed, otherwise we would have $\hat{h}(A) = \hat{h}(\varphi_q(A)) = \hat{h}([a_q/2](A)) = p^2\hat{h}(A)$ by properties of the Néron-Tate height and since $a_q/2 = \pm p$. This implies $\hat{h}(A) = 0$ and so $A \in E_{\mathrm{tors}}$ by Kronecker's Theorem, contradicting our hypothesis.

The parallelogram equality implies

$$\hat{h}(B) \leq \hat{h}(\varphi_q(A) - [a_q/2](A)) + h(\varphi_q(A) + [a_q/2](A)) = 2\hat{h}(\varphi_q(A)) + 2\hat{h}([a_q/2](A))$$

and we deduce $\hat{h}(B) \leq 2(p^2+1)\hat{h}(A)$, as desired.

As in the proof of Lemma 5.1 we see that the restriction of φ_q lies in the center of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$. This observation together with (8.2) yields

$$\lambda_{\sigma^{-1}v}(B) = \lambda_v(\sigma(\varphi_q(A)) - \sigma([a_q/2](A))) = \lambda_v(\varphi_q(\sigma(A)) - [a_q/2](\sigma(A)))$$

and $\varphi_q(\sigma(A)) \neq [a_q/2](\sigma(A))$. So $\lambda_{\sigma^{-1}v}(B) \geq (\log p)/2$ by Lemma 8.3. As σ varies over the elements of $\mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ we obtain any place above p as some $\sigma^{-1}v$.

We recall (5.5). Summing up the local heights over all places above p with the correct multiplicities and dividing by $[\mathbf{Q}(E[N]) : \mathbf{Q}]$ yields

$$\hat{h}_p(B) \geq \frac{1}{2}\log p. \qquad \square$$

Now we begin tackling the unramified case.

Lemma 8.6. *We assume $p|N$ and let $n \geq 1$ be the greatest integer with $p^n|N$. If $A \in E(\mathbf{Q}(E[N]))$ satisfies $[Q(n)](A) \notin E(\mathbf{Q}_q(E[N/p]))$, there exists a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with $\hat{h}(B) \leq 4\hat{h}(A)$ and*

$$\hat{h}_p(B) \geq \frac{\log p}{2p^6}.$$

Proof. By hypothesis there is $\psi \in \mathrm{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N/p]))$ such that $\psi([Q(n)](A)) \neq [Q(n)](A)$. It is convenient to identify ψ with its restriction to $\mathbf{Q}(E[N])$. We take the point from the assertion to be $B = \psi(A) - A$. The fact that this is not a torsion point follows from Lemma 8.2. Moreover, the parallelogram equality implies $\hat{h}(B) \leq 2\hat{h}(\psi(A)) + 2\hat{h}(A) = 4\hat{h}(A)$.

We now prove the lower bound for $\hat{h}_p(B)$. The centralizer of ψ in the global Galois group is the subgroup

$$G = \{\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q});\ \sigma\psi\sigma^{-1} = \psi\}.$$

For any $\sigma \in G$ we have

$$\lambda_{\sigma^{-1}v}(B) = \lambda_v((\sigma\psi)(A) - \sigma(A)) = \lambda_v((\psi\sigma)(A) - \sigma(A))$$

and $(\psi\sigma)(A) \neq \sigma(A)$. So Lemma 8.4 applied to $\sigma(A)$ yields

$$\lambda_{\sigma^{-1}v}(B) \geq \frac{\log p}{2(p^2-1)}. \tag{8.5}$$

We soon show that (8.5) contributes in a significant manner to the partial height $\hat{h}_p(B)$. This will follow since the orbit of v under G is sufficiently large. On the other hand, if w is any place of $\mathbf{Q}(E[N])$ with $w|p$, then $\lambda_w(B) \geq 0$ since E has good reduction at p. Thus

$$\begin{aligned}\hat{h}_p(B) &= \frac{1}{[\mathbf{Q}(E[N]):\mathbf{Q}]}\sum_{w|p} d_w\lambda_w(B)\\ &\geq \frac{1}{[\mathbf{Q}(E[N]):\mathbf{Q}]}\sum_{w\in Gv} d_w\lambda_w(B)\\ &\geq \frac{1}{[\mathbf{Q}(E[N]):\mathbf{Q}]}\frac{\log p}{2(p^2-1)}d_v\#Gv\\ &\geq \frac{\log p}{2(p^2-1)p^4}\end{aligned}$$

where in the final inequality we used the lower bound for $\#Gv$ from Lemma 5.2. □

We treat the tamely ramified case $p^2 \nmid N$ as in Lemma 6.3.

Lemma 8.7. *We assume $N \in \mathbf{N}$ with $p^2 \nmid N$. If $A \in \mathbf{Q}(E[N]) \smallsetminus E_{\mathrm{tors}}$ there exists a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with $\hat{h}(B) \leq 2p^{10}\hat{h}(A)$ and*

$$\hat{h}_p(B) \geq \frac{\log p}{2p^6}$$

Proof. We may assume $p|N$.

First, let us suppose that some conjugate A' of A over $\mathbf{Q}$ satisfies $[Q(1)](A') = [q(q-1)](A') \notin E(\mathbf{Q}_q(E[N/p]))$. Then Lemma 8.6 applied to this conjugate provides a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with $\hat{h}(B) \leq 4\hat{h}(A') = 4\hat{h}(A)$ and $\hat{h}_p(B) \geq (\log p)/(2p^6)$. The first inequality is clearly more than what we claim.

So we may assume that $\sigma([q(q-1)](A)) = [q(q-1)](\sigma(A)) \in E(\mathbf{Q}_q(E[N/p])$ for all $\sigma \in \mathrm{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$. We apply Lemma 6.2 to the coordinates of $[q(q-1)](A)$ with respect to our Weierstrass model. The point $[q(q-1)](A)$ actually lies in $E(\mathbf{Q}(E[N/p]))$. Since N/p is coprime to p, Lemma 8.5 yields a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with

$$\hat{h}(B) \leq 2(p^2+1)\hat{h}([q(q-1)](A)) = 2(p^2+1)p^4(p^2-1)^2\hat{h}(A) \leq 2p^{10}\hat{h}(A)$$

and $\hat{h}_p(B) \geq (\log p)/2$. □

We mimic the argument in Proposition 1 to obtain its counterpart in the elliptic curve setting.

Proposition 2. *Suppose E does not have complex multiplication. There exists a prime $p \geq 5$ depending only on E with the following property. If $A \in E(\mathbf{Q}(E_{\text{tors}})) \smallsetminus E_{\text{tors}}$ there is a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with $\hat{h}(B) \leq 20p^{10}\hat{h}(A)$ and*

$$\hat{h}_p(B) \geq \frac{\log p}{2p^6}.$$

Proof. We argue as in the proof of Proposition 1 to see that there is a prime p satisfying (P1) and (P2).

The point A from the hypothesis lies in $E(\mathbf{Q}(E[N]))$ with $N = p^n M$ where $M \in \mathbf{N}$ is coprime to p and n is a non-negative integer. Let σ_2 be an automorphism coming from Lemma 6.4 and define

$$C = \sigma_2(A) - [2](A) \in E(\mathbf{Q}(E[N])).$$

The parallelogram equality and other basic properties of the Néron-Tate height give

$$\hat{h}(C) \leq 2\hat{h}(\sigma_2(A)) + 2\hat{h}([2](A)) = 10\hat{h}(A). \tag{8.6}$$

We fix the least integer $n' \geq 0$ such that $C \in E(\mathbf{Q}(E[p^{n'}M]))$. Of course $n' \leq n$. For brevity, we write $N' = p^{n'}M$.

If $n' \leq 1$ then we can apply Lemma 8.7 to C if we can show that C is not a torsion point. Assuming the contrary we get $\hat{h}(A) = \hat{h}(\sigma_2(A)) = \hat{h}([2](A)) = 4\hat{h}(A)$ by properties of the Néron-Tate height. Hence $\hat{h}(A) = 0$ meaning that A is itself a torsion point by Kronecker's Theorem. But this contradicts the hypothesis. By Lemma 8.7 we obtain a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with a lower bound for $\hat{h}_p(B)$ as in the current lemma. Moreover, B satisfies

$$\hat{h}(B) \leq 2p^{10}\hat{h}(C) \leq 20p^{10}\hat{h}(A).$$

by (8.6). This completes the proof if $n' \leq 1$.

Now let us assume $n' \geq 2$. By Lemma 6.2 applied to the coordinates of A and since n' is minimal, there exists $\sigma \in \text{Gal}(\mathbf{Q}(E[N])/\mathbf{Q})$ with $C' = \sigma(C) \in E(\mathbf{Q}(E[N'])) \smallsetminus E(\mathbf{Q}_q(E[N'/p]))$. We choose a witness $\psi \in \text{Gal}(\mathbf{Q}_q(E[N])/\mathbf{Q}_q(E[N'/p]))$ testifying $\psi(C') \neq C'$.

We set $A' = \sigma(A)$ and obtain

$$C' = \sigma_2(A') - [2](A') \in E(\mathbf{Q}(E[N'])) \tag{8.7}$$

because σ_2 and σ commute.

In order to apply Lemma 8.6 to C' we must show $[Q(n')](C') = [q](C') \notin E(\mathbf{Q}_q(E[N'/p]))$. We suppose the contrary is true and derive a contradiction. Then

$$\psi(C') - C' = T \in E[q] \smallsetminus \{0\}. \tag{8.8}$$

We apply ψ to (8.7) and use the fact that it commutes with σ_2 to obtain

$$C' + T = \psi(C') = \sigma_2(\psi(A')) - [2](\psi(A')).$$

We set $P = \psi(A') - A' \in E(\mathbf{Q}(E[N]))$. A short calculation involving (8.7) gives $T = \sigma_2(P) - [2](P)$.

As we have often seen, T being torsion implies $\hat{h}(P) = \hat{h}(\sigma_2(P)) = \hat{h}([2](P)) = 4\hat{h}(P)$. Hence $\hat{h}(P) = 0$ and thus P is a torsion point too. We fix $\widetilde{M} \in \mathbf{N}$ coprime to p such that $[\widetilde{M}](P) \in E[p^\infty]$. So $[\widetilde{M}](P)$ has order dividing p^n by Lemma 8.1. By construction $\sigma_2([\widetilde{M}](P)) = [2\widetilde{M}](P)$ and so $\sigma_2(P) = [2](P) + S$ with $S \in E[\widetilde{M}]$. We substitute $\psi(A') - A'$ for P to get

$$\sigma_2(\psi(A')) - \sigma_2(A') = [2](\psi(A')) - [2](A') + S.$$

Recall that σ_2 commutes with ψ, hence

$$\psi(C') = \psi(\sigma_2(A') - [2](A')) = \sigma_2(A') - [2](A') + S = C' + S.$$

We recall (8.8) and find $S = T \in E[q] \cap E[\widetilde{M}]$. Hence $T = 0$ since q and $\widetilde{M}$ are coprime. This contradicts the choice of T and we must have $[q](C') \notin E(\mathbf{Q}_q(E[N'/p]))$.

Now we may apply Lemma 8.6 to C'. It gives us a non-torsion point $B \in E(\overline{\mathbf{Q}})$ with

$$\hat{h}_p(B) \geq \frac{\log p}{2p^6}$$

and $\hat{h}(B) \leq 4\hat{h}(C')$. But $\hat{h}(C') = \hat{h}(C)$ and we recall (8.6) to obtain $\hat{h}(B) \leq 40\hat{h}(A) \leq 20p^{10}\hat{h}(A)$, as desired. □

Suppose B and p are as in the previous proposition. The next lemma relies on Archimedean and non-Archimedean equidistribution properties alluded to in the introduction. We use it to show that the partial height functions $\hat{h}_\ell(B)$ at places $\ell \neq p$ are negligible if B has small Néron-Tate height.

Lemma 8.8. *Let $A_1, A_2, \ldots$ be a sequence of non-torsion points in $E(\overline{\mathbf{Q}})$ with $\lim_{k\to\infty} \hat{h}(A_k) = 0$. If ℓ is a place of $\mathbf{Q}$, then*

$$\liminf_{k\to\infty} \hat{h}_\ell(A_k) \geq 0.$$

Moreover, if ℓ is finite and does not divide the denominator of the j-invariant of E, then $\hat{h}_\ell(A_k) \geq 0$.

Proof. Say $A \in E(\overline{\mathbf{Q}}) \smallsetminus \{0\}$. We first treat the case $\ell = \infty$. Then

$$\hat{h}_\infty(A) = \frac{1}{[\mathbf{Q}(A) : \mathbf{Q}]} \sum_\sigma \lambda_\infty(\sigma(A))$$

where σ runs over all field embeddings $\mathbf{Q}(A) \to \mathbf{C}$, Recall that $\lambda_\infty : E(\mathbf{C}) \smallsetminus \{0\} \to \mathbf{R}$ is a local height function. It is continuous, but unbounded as the argument approaches $0 \in E(\mathbf{C})$. So we cannot refer to Szpiro, Ullmo, and Zhang's Theorem 4 directly. Rather we truncate the local height using a parameter $m \in \mathbf{N}$. More precisely, we define a continuous function $\lambda_{\infty,m} : E(\mathbf{C}) \to \mathbf{R}$ by setting

$$\lambda_{\infty,m}(A) = \min\{m, \lambda_\infty(A)\}$$

for all $A \in E(\mathbf{C}) \smallsetminus \{0\}$ and $\lambda_{\infty,m}(0) = m$. Now $\lambda_{\infty,m}$ is clearly bounded from above and moreover continuous. By a well-known fact that can be deduced from (8.1), λ_∞ is also bounded from below. Theorem 4 applies to $\lambda_{\infty,m}$ and the right-hand side of

$$\hat{h}_\infty(A_k) \geq \frac{1}{[\mathbf{Q}(A) : \mathbf{Q}]} \sum_\sigma \lambda_{\infty,m}(\sigma(A_k))$$

converges to $a_m = \int \lambda_{\infty,m}\mu_{E,\infty}$ as $k \to \infty$. Therefore, $\liminf_{k\to\infty} \hat{h}_\infty(A_k) \geq a_m$. The functions $\lambda_{\infty,m}$ are pointwise increasing in m with pointwise limit λ_∞ on $E(\mathbf{C}) \smallsetminus \{0\}$. By the Monotone Convergence Theorem λ_∞ is measurable on $E(\mathbf{C})$, its value at 0 being irrelevant, with $\lim_{m\to\infty} a_m = \int \lambda_\infty \mu_{E,\infty}$. The lemma follows for $\ell = \infty$ if we can show

$$\int \lambda_\infty \mu_{E,\infty} = 0. \tag{8.9}$$

Indeed, this is well-known but we provide a short proof. We expressed λ_∞ in (8.1) as an infinite series. Let $\tau \in \mathbf{C}$ have positive imaginary part and $q = e^{2\pi i\tau}$. By the Dominant Convergence Theorem it suffices to show that the integral over

$$\{z = x + y\tau;\ x, y \in [0,1)\} \subset \mathbf{C}.$$

of each term vanishes. Elementary calculus shows

$$\int_0^1 b_2(y)dy = \int_0^1 \left(y^2 - y + \frac{1}{6}\right) dy = 0.$$

Suppose $n \geq 1$. Then

$$\int_{[0,1)^2} \log|1-q^n e^{\pm 2\pi i(x+y\tau)}|dxdy = \int_{[0,1)^2} \log|e^{\mp 2\pi i x} - e^{2\pi i\tau(n\pm y)}|dxdy = \int_0^1 \log\max\{1, |e^{2\pi i\tau(n\pm y)}|\}dy$$

by Jensen's Formula. But $|e^{2\pi i\tau(n\pm y)}| = e^{-2\pi \mathrm{Im}(\tau)(n\pm y)} \leq 1$ since $\mathrm{Im}(\tau) > 0$ and $y \in [0,1)$. So $\int_{[0,1)^2} \log|1 - q^n e^{\pm 2\pi i(x+y\tau)}|dxdy = 0$. Along the same lines we find $\int_0^1 b_2(-y)dy = \int_{[0,1)^2} \log|1-u|dxdy = 0$. So (8.9) holds true.

Next we treat the case when ℓ is a finite place of $\mathbf{Q}$.

There exists a finite Galois extension $F/\mathbf{Q}$ such that E considered as an elliptic curve defined over F has either good or split multiplicative reduction at all finite places. Let $p_1, \ldots, p_s$ be precisely the primes appearing in the denominator of the j-invariant of E.

Suppose v is a finite place of F. By the basic theory of elliptic curves the reduction type of E is determined as follows. If $v|p_i$ for some i, then E has split multiplication reduction at v. If $v \nmid p_i$ for all i, then E has good reduction at v.

Suppose ℓ is not among the p_i. Then λ_v is non-negative for all $v|\ell$ by (8.2). Therefore, we obtain $\hat{h}_\ell(A) \geq 0$ for all $A \in E(\overline{\mathbf{Q}}) \smallsetminus \{0\}$. The second statement of this lemma follows and the lower bound for the limes inferior is trivial.

Finally, let us assume $\ell = p_i$ for some i. Let v be a place of F above ℓ and $\overline{F_v}$ a fixed algebraic closure of F_v.

Suppose $A \in E(\overline{\mathbf{Q}}) \smallsetminus \{0\}$ and let $K = F(A)$. Since λ_v is invariant under the action of $\mathrm{Gal}(\overline{F_v}/F_v)$ we have

$$\hat{h}_\ell(A) = \frac{1}{[F:\mathbf{Q}]}\sum_{\sigma'} \frac{1}{[K:F]}\sum_{\sigma} \lambda_v(\sigma(A)) \tag{8.10}$$

where $\sigma' : F \to \overline{F_v}$ and $\sigma : K \to \overline{F_v}$ run over all field embeddings with $\sigma|_F = \sigma'$.

Let us fix a field embedding $\sigma' : F \to \overline{F_v}$. We consider the Tate uniformization $\overline{F_v}^\times \to E(\overline{F_v})$ and let $q_v \in F_v^\times$ denote the associated parameter. For any σ as above we fix $u_\sigma \in \overline{F_v}^\times$ with $|q|_v < |u_\sigma|_v \leq 1$ in the preimage of $\sigma(A)$. Recall that $l_v(A) =$

$\log|u|_v/\log|q|_v + \mathbf{Z} \in \mathbf{R}/\mathbf{Z}$. We define $\overline{b_2}$ to be $b_2|_{[0,1)}$ extended periodically to $\mathbf{R}$. Then $\overline{b_2}(l_v(A))$ is well-defined and by (8.3) we get

$$\lambda_v(\sigma(A)) = -\frac{1}{2}\overline{b_2}\left(l_v(A)\right)\log|q|_v - \log|1-u_\sigma|_v \geq -\frac{1}{2}\overline{b_2}\left(l_v(A)\right)\log|q|_v \tag{8.11}$$

since $|1-u_\sigma|_v \leq 1$.

Now we can apply Chambert-Loir's Theorem 5 to get

$$\lim_{k\to\infty} -\frac{1}{2}\frac{1}{[F(A_k):F]}\sum_{\sigma:F(A_k)\to\overline{F_v}} \overline{b_2}\left(l_v(A_k)\right) = -\frac{1}{2}\int \overline{b_2}\left(x\right)\mu_{\mathbf{R}/\mathbf{Z}}.$$

The integral on the left is $\int_0^1 b_2(t)dt$ and hence vanishes as in the Archimedean case. We recall (8.11) and (8.10) to derive

$$\liminf_{k\to\infty} \hat{h}_\ell(A_k) \geq 0. \qquad \square$$

Proof of Theorem 2. We follow a similar argumentation as in the proof of Theorem 1. If E has complex multiplication by an order in an imaginary quadratic number field K, then $K(E_{\mathrm{tors}})$ is an abelian extension of K. In this case the theorem follows from Baker's Theorem 1.1 [4].

So let us suppose that E does not have complex multiplication.

We prove the theorem by contradiction. So let $A_1, A_2, \ldots$ be a sequence of non-torsion points in $E(\mathbf{Q}(E_{\mathrm{tors}}))$ with $\lim_{k\to\infty}\hat{h}(A_k) = 0$. Proposition 2 yields a prime p and a new sequence $B_1, B_2, \ldots$ of non-torsion points in $E(\overline{\mathbf{Q}})$ with $\lim_{k\to\infty}\hat{h}(B_k) = 0$ but

$$\hat{h}_p(B_k) \geq \frac{\log p}{2p^6}.$$

Therefore,

$$\hat{h}(B_k) \geq \frac{\log p}{2p^6} + \sum_{\ell\neq p}\hat{h}_\ell(B_k)$$

where ℓ ranges over all places of $\mathbf{Q}$ other than p.

By the second statement of Lemma 8.8 we may omit all finite places ℓ that do not appear in the denominator of the j-invariant of E in the sum on the right. So the limes inferior of the right-hand side is at least $(\log p)/(2p^6)$ by the first claim in Lemma 8.8. That of the left-hand side is of course zero and this is a contradiction. □

References

1. F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272.
2. F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), no. 3, 711–727.
3. ______, *A uniform relative Dobrowolski's lower bound over abelian extensions*, Bull. Lond. Math. Soc. **42** (2010), no. 3, 489–498.
4. M.H. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Not. (2003), no. 29, 1571–1589.
5. M.H. Baker and C. Petsche, *Global discrepancy and small points on elliptic curves*, Int. Math. Res. Not. (2005), no. 61, 3791–3834.
6. Y. Bilu, *Limit distribution of small points on algebraic tori*, Duke Math. J. **89** (1997), no. 3, 465–476.
7. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.

8. E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **12** (2001), 5–14 (2002).
9. A. Chambert-Loir, *Mesures et équidistribution sur les espaces de Berkovich*, J. Reine Angew. Math. **595** (2006), 215–235.
10. ———, *Relations de dépendance et intersections exceptionnelles (dependence relations and exceptional intersections)*, Séminaire Bourbaki, 63e année, 2010-11, Exposé n. 1032 (2011).
11. N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567.
12. D. Husemöller, *Elliptic Curves*, Springer, 2004.
13. J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.
14. N. Ratazzi, *Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe*, Int. Math. Res. Not. (2004), no. 58, 3121–3152.
15. A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399.
16. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
17. J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
18. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
19. ———, *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory **104** (2004), no. 2, 353–372.
20. L. Szpiro, E. Ullmo, and S. Zhang, *Équirépartition des petits points*, Invent. Math. **127** (1997), no. 2, 337–347.
21. S. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165.

Philipp Habegger, Johann Wolfgang Goethe-Universität, Robert-Mayer-Str. 6-8, 60325 Frankfurt am Main, Germany, habegger@math.uni-frankfurt.de